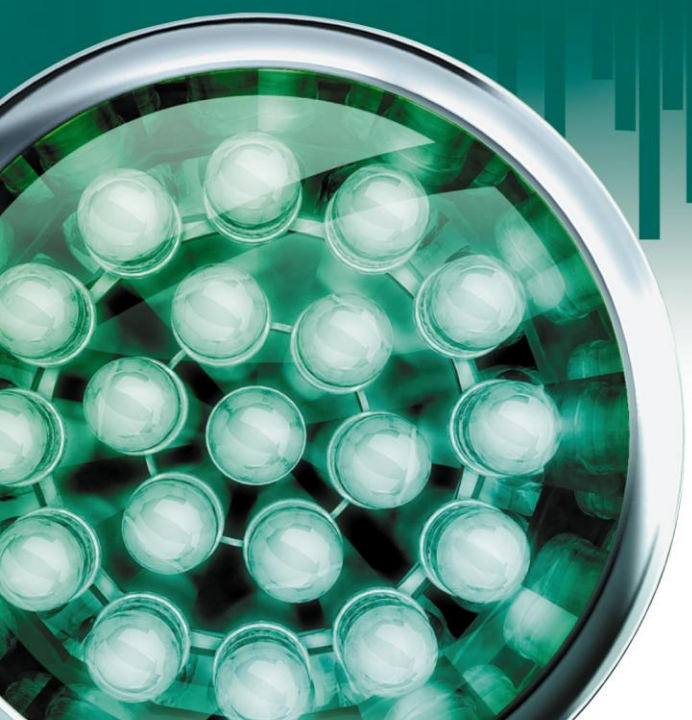
Kaspersky Mobile Security 9.0

BENUTZERHANDBUCH

PROGRAMMVERSION: 9.0



KASPERSKY lab

Sehr geehrte Benutzerinnen und Benutzer!

Vielen Dank, dass Sie sich für unser Produkt entschieden haben. Wir hoffen, dass Ihnen diese Dokumentation bei der Arbeit behilflich sein und auf die mit dem Produkt verbundenen Fragen antworten wird.

Die Materialien dürfen nur mit schriftlicher Einwilligung von Kaspersky Lab ZAO auf elektronische, mechanische oder sonstige Weise kopiert, verbreitet oder übersetzt werden.

Das Dokument und die darin enthaltenen Bilder sind ausschließlich für informative, nicht gewerbliche und persönliche Zwecke bestimmt.

Das Dokument kann zukünftig ohne besondere Ankündigung geändert werden. Die aktuelle Version des Dokuments steht auf der Seite von Kaspersky Lab unter der Adresse http://www.kaspersky.com/de/docs zur Verfügung.

Kaspersky Lab ZAO übernimmt keine Haftung für Inhalt, Qualität, Aktualität und Richtigkeit von in diesem Dokument verwendeten Materialien, deren Rechte bei anderen Eigentümern liegen, sowie für möglichen Schaden, der mit der Verwendung dieser Materialien verbunden ist.

In diesem Dokument werden registrierte oder nicht registrierte Markenzeichen verwendet, die Eigentum der rechtmäßigen Besitzer sind.

Redaktionsdatum: 04.02.2010

© 1997-2010 Kaspersky Lab ZAO

http://www.kaspersky.de
http://support.kaspersky.de

ENDNUTZER-LIZENZVERTRAG FÜR KASPERSKY LAB SOFTWARE

WICHTIGER RECHTLICHER HINWEIS AN ALLE NUTZER: LESEN SIE FOLGENDE RECHTLICHE VEREINBARUNG SORGFÄLTIG DURCH, BEVOR SIE DIE SOFTWARE NUTZEN.

INDEM SIE IM LIZENZVERTRAG-FENSTER AUF DIE SCHALTFLÄCHE AKZEPTIEREN KLICKEN ODER EIN ENTSPRECHENDES ZEICHEN BZW. ENTSPRECHENDE ZEICHEN EINGEBEN, ERKLÄREN SIE SICH MIT DER EINHALTUNG DER GESCHÄFTSBEDINGUNGEN DIESES VERTRAGS EINVERSTANDEN. **DIESE AKTION KONSTITUIERT EIN BEKENNTNIS IHRER SIGNATUR UND SIE STIMMEN DIESER VEREINBARUNG, UND DASS SIE EINE PARTEI DIESER VEREINBARUNG WERDEN, ZU UND ERKLÄREN SICH WEITERHIN EINVERSTANDEN, DASS DIESE VEREINBARUNG, WIE JEDWEDE ANDERE SCHRIFTLICHE, AUSGEHANDELTE UND DURCH SIE UNTERZEICHNETE VEREINBARUNG AUCH, VOLLSTRECKBAR IST.** SOLLTEN SIE MIT DEN GESCHÄFTSBEDINGUNGEN DIESER VEREINBARUNG NICHT EINVERSTANDEN SEIN, BEENDEN SIE DIE INSTALLATION DER SOFTWARE BZW. INSTALLIEREN SIE SIE NICHT.

NACHDEM SIE IM LIZENZVERTRAG-FENSTER AUF DIE SCHALTFLÄCHE AKZEPTIEREN GEKLICKT ODER EIN ENTSPRECHENDES ZEICHEN BZW. ENTSPRECHENDE ZEICHEN EINGEGEBEN HABEN, SIND SIE BERECHTIGT, DIE SOFTWARE IM EINKLANG MIT DEN GESCHÄFTSBEDINGUNGEN DIESER VEREINBARUNG ZU NUTZEN.

1. Definitionen

1.1. **Software** bezeichnet Software einschließlich aller Updates und zugehöriger Materialien.

1.2. **Rechtsinhaber** (Inhaber aller Rechte an der Software, ob exklusiv oder anderweitig) bezeichnet Kaspersky Lab ZAO, ein gemäß den Gesetzen der Russischen Föderation amtlich eingetragenes Unternehmen.

1.3. **Computer** bezeichnet/bezeichnen Hardware, einschließlich von PCs, Laptops, Workstations, PDAs, Smart Phones, tragbaren oder sonstigen elektronischen Geräten, für welche die Software konzipiert war und auf denen die Software installiert und/oder verwendet werden wird.

1.4. **Endnutzer (Sie)** bezeichnet eine bzw. mehrere Personen, die die Software in eigenem Namen installieren oder nutzen, oder die eine Software-Kopie rechtmäßig nutzt/nutzen, oder, falls die Software im Namen einer Organisation heruntergeladen oder installiert wurde, wie etwa einem Arbeitgeber, bezeichnet der Begriff *„Sie“* weiterhin jene Organisation, für die die Software heruntergeladen oder installiert wird, und es wird hiermit erklärt, dass eine solche Organisation die diese Vereinbarung akzeptierende Person autorisiert hat, dies in ihrem Namen zu tun. Im Sinne dieses Lizenzvertrags beinhaltet der Begriff *„Organisation“* ohne Einschränkungen jedwede Partnerschaft, GmbH, Gesellschaft, Vereinigung, Aktiengesellschaft, Treuhandgesellschaft, Gemeinschaftsunternehmen, Arbeitsorganisation, nicht eingetragene Organisation oder staatliche Behörde.

1.5. **Partner** bezeichnet Organisationen oder Personen, die die Software auf Grundlage eines Vertrags und einer mit dem Rechtsinhaber vereinbarten Lizenz vertreiben.

1.6. **Update(s)** bezeichnet/n alle Upgrades, Korrekturen, Patches, Erweiterungen, Reparaturen, Modifikationen, Kopien, Ergänzungen oder Wartungs-Softwarepakete usw.

1.7. **Benutzerhandbuch** bezeichnet die Bedienungsanleitung, die Administrator-Anleitung, ein Nachschlagewerk und ähnliche erläuternde oder sonstige Materialien.

2. Lizenzgewährung

2.1. Der Rechtsinhaber gewährt Ihnen hiermit eine nicht-ausschließliche Lizenz zur Speicherung, zum Laden, zur Installation, Ausführung und Darstellung (zur „Nutzung“) der Software auf einer festgelegten Anzahl von Computern zur Unterstützung des Schutzes Ihres Computers, auf dem die Software installiert ist, vor im Nutzerhandbuch beschriebenen Bedrohungen gemäß den technischen, im Benutzerhandbuch beschriebenen Anforderungen und im Einklang mit den Geschäftsbedingungen dieses Vertrags (die „Lizenz“). Sie erkennen diese Lizenz an.

Testversion. Sollten Sie eine Testversion der Software erhalten, heruntergeladen und/oder installiert haben und sollte Ihnen hiermit eine Evaluierungslizenz für die Software gewährt worden sein, dürfen Sie die Software ab dem Datum der ersten Installation nur zu Evaluierungszwecken verwenden, und zwar ausschließlich während der einzigen geltenden Evaluierungsperiode, außer wie anderweitig angegeben. Jegliche Nutzung der Software zu anderen Zwecken oder über die geltende Evaluierungsperiode hinaus ist strikt untersagt.

Software für mehrere Umgebungen; Mehrsprachige Software; Dual-Medien-Software; Mehrere Kopien; Softwarebündel. Wenn Sie verschiedene Versionen der Software oder verschiedene Sprachausgaben der Software verwenden, wenn Sie die Software auf mehreren Medien erhalten, wenn Sie anderweitig mehrere Kopien der Software erhalten oder wenn Sie die Software mit einer anderen Software gebündelt erhalten

sollten, entspricht die insgesamt zulässige Anzahl Ihrer Computer, auf denen alle Versionen der Software installiert sind, der Anzahl der in den Lizenzen, die Sie vom Rechtsinhaber bezogen haben, bezeichneten Computern, und jede erworbene Lizenz berechtigt Sie zur Installation und Nutzung der Software auf dieser Anzahl von Computern entsprechend den Festlegungen in den Klauseln 2.2 und 2.3, *außer die* Lizenzbedingungen sehen eine anderweitige Regelung vor.

2.2. Wenn die Software auf einem physischen Medium erworben wurde, haben Sie das Recht, die Software zum Schutz einer solchen Anzahl von Computern zu verwenden, die auf der Softwareverpackung oder in der Zusatzvereinbarung festgelegt ist.

2.3. Wenn die Software über das Internet erworben wurde, haben Sie das Recht, die Software zum Schutz einer solchen Anzahl von Computern zu verwenden, die genannt wurde, als Sie die Lizenz für die Software gekauft haben, bzw. jene in der Zusatzvereinbarung festgelegte Anzahl von Computern.

2.4. Sie haben das Recht, eine Kopie der Software anzufertigen, und zwar ausschließlich zu Sicherungszwecken und nur, um die rechtmäßig in Ihrem Besitz befindliche Kopie zu ersetzen, sollte eine solche Kopie verloren gehen, zerstört oder unbrauchbar werden. Diese Sicherungskopie kann nicht zu anderen Zwecken verwendet werden und muss zerstört werden, wenn Sie das Recht verlieren, die Software zu nutzen oder wenn Ihre Lizenz abläuft oder aus irgendeinem Grund im Einklang mit der gültigen Gesetzgebung im Land Ihres Wohnsitzes oder in dem Land, in dem Sie die Software nutzen, gekündigt werden sollte.

2.5. Ab dem Zeitpunkt der Aktivierung der Software bzw. Installation der Lizenzschlüsseldatei (mit Ausnahme einer Testversion der Software) haben Sie das Recht, folgende Dienstleistungen für den auf der Softwareverpackung (falls Sie Software auf einem physischen Medium erworben haben) oder während des Kaufs (falls die Software über das Internet erworben wurde) festgelegten Zeitraum zu beziehen:

- Updates der Software über das Internet, wenn und wie der Rechtsinhaber diese auf seiner Webseite oder mittels anderer Online-Dienste veröffentlicht. Jedwede Updates, die Sie erhalten, werden Teil der Software und die Geschäftsbedingungen dieses Vertrags gelten für diese;
- Technische Unterstützung über das Internet sowie technische Unterstützung über die Telefon-Hotline.

3. Aktivierung und Zeitraum

3.1. Falls Sie Modifikationen an Ihrem Computer oder an der darauf installierten Software anderer Anbieter vornehmen, kann der Rechtsinhaber von Ihnen verlangen, die Aktivierung der Software bzw. die Installation der Lizenzschlüsseldatei zu wiederholen. Der Rechtsinhaber behält sich das Recht vor, jegliche Mittel und Verifizierungsverfahren zu nutzen, um die Gültigkeit der Lizenz und/oder die Rechtmäßigkeit einer Kopie der Software, die auf Ihrem Computer installiert und/oder genutzt wird, zu verifizieren.

3.2. Falls die Software auf einem physischen Medium erworben wurde, kann die Software nach Ihrer Annahme dieses Vertrags mit Beginn ab dem Zeitpunkt der Annahme dieses Vertrags für die auf der Verpackung bezeichnete oder in der Zusatzvereinbarung genannte Periode genutzt werden.

3.3. Falls die Software über das Internet erworben wurde, kann die Software nach Ihrer Annahme dieses Vertrags für die während des Kaufs oder in der Zusatzvereinbarung bezeichnete Zeitdauer genutzt werden.

3.4. Sie haben das Recht, eine Testversion der Software zu nutzen, und zwar gemäß der Festlegung in Klausel 2.1 und ohne jedwede Gebühr für die einzelne geltende Evaluierungsperiode (30 Tage) ab dem Zeitpunkt der Aktivierung der Software im Einklang mit diesem Vertrag, *und zwar unter der Bedingung, dass* die Testversion Ihnen nicht das Recht auf Updates und technische Unterstützung über das Internet und technische Unterstützung über die Telefon-Hotline einräumt. Wenn der Rechtsinhaber für die einzelne geltende Evaluierungsperiode einen anderen Zeitraum festlegt, erhalten Sie darüber eine Mitteilung.

3.5. Ihre Lizenz zur Nutzung der Software beschränkt sich auf den in den Klauseln 3.2 oder 3.3 (je nach Anwendbarkeit) bezeichneten Zeitraum. Die verbleibende Zeitdauer kann auf die im Benutzerhandbuch beschriebene Weise abgefragt werden.

3.6. Haben Sie die Software zur Nutzung auf mehr als einem Computer erworben, beginnt der Zeitraum, auf den Ihre Lizenz zur Nutzung der Software begrenzt ist, am Tag der Aktivierung der Software bzw. der Installation der Lizenzschlüsseldatei auf dem ersten Computer.

3.7. Unbeschadet anderer Rechtsmittel laut Gesetz oder Billigkeitsrecht, zu denen der Rechtsinhaber im Falle eines Verstoßes gegen die Geschäftsbedingungen dieses Vertrags durch Sie berechtigt ist, ist der Rechtsinhaber jederzeit, ohne Sie benachrichtigen zu müssen, dazu berechtigt, diese Lizenz zur Nutzung der Software zu kündigen, und zwar ohne den Verkaufspreis oder einen Teil davon zurückzuerstatten.

3.8. Sie stimmen zu, dass Sie bei der Nutzung der Software sowie bei der Verwendung jedweder Berichte oder Informationen, die sich als Ergebnis der Nutzung der Software ableiten, alle geltenden internationalen, nationalen, staatlichen, regionalen und lokalen Gesetze sowie gesetzlichen Bestimmungen, einschließlich (und ohne Beschränkung) Datenschutz-, Urheber-, Exportkontroll- und Verfassungsrecht, einhalten werden.

3.9. Außer wenn anderweitig hierin festgelegt, dürfen Sie keines der Rechte, die Ihnen unter diesem Vertrag gewährt werden, bzw. keine Ihrer hieraus entstehenden Pflichten übertragen oder abtreten.

4. Technische Unterstützung

Die in Klausel 2.5 dieses Vertrags erläuterte technische Unterstützung wird Ihnen gewährt, wenn das neueste Update der Software installiert wird (außer im Fall einer Testversion der Software).
Technischer Support: http://support.kaspersky.com

5. Beschränkungen

5.1. Sie werden die Software nicht emulieren, klonen, vermieten, verleihen, leasen, verkaufen, modifizieren, dekompilieren oder zurückentwickeln oder disassemblieren oder Arbeiten auf Grundlage der Software oder eines Teils davon ableiten, jedoch mit der einzigen Ausnahme eines Ihnen durch geltende Gesetzgebung gewährten Rechts, von dem keine Rücktretung möglich ist, und Sie werden in keiner anderen Form irgendeinen Teil der Software in menschlich lesbare Form umwandeln oder die lizenzierte Software oder irgendeine Teilmenge der lizenzierten Software übertragen, noch irgendeiner Drittpartei gestatten, dies zu tun, außer im Umfang vorangegangener Einschränkungen, die ausdrücklich durch geltendes Recht untersagt sind. Weder Binärcode noch Quellcode der Software dürfen verwendet oder zurückentwickelt werden, um den Programmalgorithmus, der proprietär ist, wiederherzustellen. Alle Rechte, die nicht ausdrücklich hierin gewährt werden, verbleiben beim Rechtsinhaber und/oder dessen Zulieferern, je nachdem, was zutrifft. Jegliche derartige nicht autorisierte Nutzung der Software kann zur sofortigen und automatischen Kündigung dieses Vertrags sowie der hierunter gewährten Lizenz und zu Ihrer straf- und/oder zivilrechtlichen Verfolgung führen.

5.2. Sie werden die Rechte zur Nutzung der Software nicht an eine Drittpartei übertragen, außer entsprechend den Bestimmungen der Zusatzvereinbarung zu diesem Vertrag.

5.3. Sie werden den Aktivierungscode und/oder die Lizenzschlüssel-Datei keinen Drittparteien verfügbar machen oder Drittparteien Zugang zum Aktivierungscode und/oder zum Lizenzschlüssel gewähren. Aktivierungscode und/oder Lizenzschlüssel werden/wird als vertrauliche Daten des Rechtsinhabers betrachtet, und Sie werden angemessene Sorgfalt zum Schutz der Vertraulichkeit des Aktivierungscodes und/oder des Lizenzschlüssels walten lassen, sofern Sie den Aktivierungscode und/oder den Lizenzschlüssel entsprechend den Bestimmungen der Zusatzvereinbarung zu diesem Vertrag an Drittparteien übertragen dürfen.

5.4. Sie werden die Software nicht an eine Drittpartei vermieten, verleasen oder verleihen.

5.5. Sie werden die Software nicht zur Erstellung von Daten oder Software verwenden, die zur Feststellung, zum Sperren oder zur Handhabung von Bedrohungen, wie im Nutzerhandbuch beschrieben, genutzt werden.

5.6. Der Rechtsinhaber hat das Recht, die Schlüsseldatei zu blockieren oder Ihre Lizenz zu kündigen, falls Sie gegen irgendwelche Geschäftsbedingungen dieses Vertrags verstoßen, und zwar ohne irgendeine Rückerstattung an Sie.

5.7. Falls Sie die Testversion der Software verwenden, sind Sie nicht berechtigt, technische Unterstützung, wie in Klausel 4 dieses Vertrags festgelegt, zu erhalten, und Sie sind ebenfalls nicht berechtigt, die Lizenz oder die Rechte zur Nutzung der Software an irgendeine Drittpartei zu übertragen.

6. Eingeschränkte Garantie und Haftungsausschluss

6.1. Der Rechtsinhaber garantiert, dass die Software im Wesentlichen im Einklang mit den im Nutzerhandbuch dargelegten Spezifikationen und Beschreibungen funktionieren wird, *jedoch vorausgesetzt,* dass eine solche eingeschränkte Garantie nicht für Folgendes gilt: (w) Mängel Ihres Computers und zugehörigen Verstoß, wofür der Rechtsinhaber ausdrücklich jedwede Gewährleistungsverantwortung ablehnt; (x) Funktionsstörungen, Defekte oder Ausfälle, resultierend aus falscher Verwendung, Missbrauch, Unfall, Nachlässigkeit, unsachgemäßer/m Installation, Betrieb oder Wartung, Diebstahl, Vandalismus, höherer Gewalt, terroristischen Akten, Stromausfällen oder -schwankungen, Unglück, Veränderung, nicht zulässiger Modifikation oder Reparaturen durch eine Partei außer dem Rechtsinhaber oder Maßnahmen einer sonstigen Drittpartei oder Aktionen ihrerseits, oder Ursachen außerhalb der Kontrolle des Rechtsinhabers; (y) jedweder Defekt, der dem Rechtsinhaber nicht durch Sie bekannt gemacht wird, sobald dies nach dem ersten Auftreten des Defekts möglich ist; und (z) Inkompatibilität, verursacht durch Hardware- und/oder Software-Komponenten, die auf Ihrem Computer installiert sind.

6.2. Sie bestätigen, akzeptieren und erkennen an, dass keine Software frei von Fehlern ist, und Sie sind angehalten, den Computer mit einer für Sie geeigneten Häufigkeit und Beständigkeit zu sichern.

6.3. Sie bestätigen, akzeptieren und anerkennen, dass dem Rechteinhaber keinerlei Verantwortung oder Haftung für die von Ihnen genehmigte Löschung von Daten entsteht. Die erwähnten Daten können jedwede persönlichen oder vertraulichen Informationen beinhalten.

6.4. Der Rechtsinhaber gibt keine Garantie, dass die Software im Fall von Verstößen gegen die Bedingungen, wie im Nutzerhandbuch oder in diesem Vertrag beschrieben, einwandfrei funktionieren wird.

6.5. Der Rechtsinhaber garantiert nicht, dass die Software einwandfrei funktionieren wird, wenn Sie nicht regelmäßig, wie in Klausel 2.5 dieses Vertrags erläutert, Updates herunterladen.

6.6. Der Rechtsinhaber garantiert keinen Schutz vor im Nutzerhandbuch beschriebenen Bedrohungen nach Ablauf der in Klausel 3.2 oder 3.3 dieses Vertrags bezeichneten Periode oder nachdem die Lizenz zur Nutzung der Software aus irgendeinem Grund gekündigt wurde.

6.7. DIE SOFTWARE WIRD OHNE MÄNGELGEWÄHR BEREITGESTELLT UND DER RECHTSINHABER GIBT KEINE ZUSICHERUNG UND KEINE GEWÄHRLEISTUNG IN BEZUG AUF IHRE NUTZUNG ODER LEISTUNG. DER RECHTSINHABER UND SEINE PARTNER GEWÄHREN AUßER DEN GARANTIEN, ZUSICHERUNGEN, BESTIMMUNGEN ODER BEDINGUNGEN, DIE DURCH GELTENDES RECHT NICHT AUSGESCHLOSSEN ODER BESCHRÄNKT WERDEN KÖNNEN, KEINE GARANTIEN, ZUSICHERUNGEN, BESTIMMUNGEN ODER BEDINGUNGEN (AUSDRÜCKLICHER ODER STILLSCHWEIGENDER NATUR, DIE ENTWEDER AUS EINER GESCHÄFTSBEZIEHUNG ODER EINEM HANDELSBRAUCH ENTSTEHEN BZW. AUS GESETZLICHEN, GEWOHNHEITSRECHTLICHTEN ODER ANDEREN VORSCHRIFTEN ABGELEITET

WERDEN) HINSICHTLICH JEDWEDER ANGELEGENHEIT, EINSCHLIEßLICH (OHNE EINSCHRÄNKUNG) VON NICHTVERLETZUNG VON RECHTEN DRITTER, MARKTGÄNGIGKEIT, BEFRIEDIGENDE QUALITÄT, INTEGRIERUNG ODER BRAUCHBARKEIT FÜR EINEN BESTIMMTEN ZWECK. SIE TRAGEN DAS GESAMTE STÖRUNGSRISIKO UND DAS GESAMTRISIKO HINSICHTLICH DER LEISTUNG UND VERANTWORTUNG FÜR DIE AUSWAHL DER SOFTWARE, UM IHRE VORGESEHENEN RESULTATE ZU ERZIELEN, UND FÜR DIE INSTALLATION SOWIE DIE NUTZUNG DER SOFTWARE UND DIE MIT IHR ERZIELTEN ERGEBNISSE. OHNE EINSCHRÄNKUNG DER VORANGEGANGENEN BESTIMMUNGEN MACHT DER RECHTSINHABER KEINE ZUSICHERUNGEN UND GIBT KEINE GEWÄHRLEISTUNG, DASS DIE SOFTWARE FEHLERFREI ODER FREI VON UNTERBRECHUNGEN ODER SONSTIGEN STÖRUNGEN IST ODER DASS DIE SOFTWARE JEDWEDE ODER ALL IHRE ANFORDERUNGEN ERFÜLLEN WIRD, UNGEACHTET DESSEN, OB GEGENÜBER DEM RECHTSINHABER OFFEN GELEGT ODER NICHT.

7. Haftungsausschluss und Haftungsbeschränkungen

INSOWEIT GESETZLICH STATTHAFT, SIND DER RECHTSINHABER UND SEINE PARTNER UNTER KEINEN UMSTÄNDEN HAFTBAR FÜR JEDWEDE SPEZIELLEN ODER BEILÄUFIGEN SCHÄDEN, STRAFZUSCHLAG ZUM SCHADENERSATZ, INDIREKTE ODER FOLGESCHÄDEN (EINSCHLIEßLICH UND NICHT BESCHRÄNKT AUF SCHÄDEN AUS VERLUST VON GEWINN ODER VERTRAULICHEN ODER SONSTIGEN INFORMATIONEN, FÜR GESCHÄFTSUNTERBRECHUNG, FÜR VERLUST VON PRIVATSPHÄRE, KORRUPTION, BESCHÄDIGUNG UND VERLUST VON DATEN ODER PROGRAMMEN, FÜR VERSÄUMNIS EINER PFLICHTERFÜLLUNG, EINSCHLIEßLICH JEDWEDER GESETZLICHER PFLICHTEN, TREUEPFLICHT ODER PFLICHT ZUR WAHRUNG ANGEMESSENER SORGFALT, FÜR NACHLÄSSIGKEIT, FÜR WIRTSCHAFTLICHEN VERLUST UND FÜR FINANZIELLEN ODER JEDWEDEN SONSTIGEN VERLUST), DIE AUS ODER AUF IRGENDEINE WEISE IM ZUSAMMENHANG MIT DER NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DER SOFTWARE, DER BEREITSTELLUNG ODER DEM VERSÄUMNIS DER BEREITSTELLUNG TECHNISCHER UNTERSTÜTZUNG ODER SONSTIGER DIENSTLEISTUNGEN, INFORMATIONEN, SOFTWARE UND ZUGEHÖRIGEM INHALT MITTELS DER SOFTWARE RESULTIEREN, ODER SICH ANDERWEITIG AUS DER NUTZUNG DER SOFTWARE ODER ANDERWEITIG UNTER BZW. IM ZUSAMMENHANG MIT EINER BESTIMMUNG DIESES VERTRAGS ERGEBEN, ODER DIE FOLGE EINES VERTRAGSBRUCHS ODER UNERLAUBTER HANDLUNG (EINSCHLIEßLICH NACHLÄSSIGKEIT, FALSCHANGABE, JEDWEDER STRIKTEN HAFTUNGSVERPFLICHTUNG ODER -PFLICHT), ODER EINER VERLETZUNG GESETZLICHER PFLICHTEN ODER DER GEWÄHRLEISTUNG DES RECHTSINHABERS ODER EINES SEINER PARTNER SIND, UND ZWAR AUCH DANN NICHT, WENN DER RECHTSINHABER ODER EINER SEINER PARTNER BEZÜGLICH DER MÖGLICHKEIT SOLCHER SCHÄDEN INFORMIERT WURDE.

SIE STIMMEN ZU, DASS IN DEM FALL, DASS DER RECHTSINHABER UND/ODER SEINE PARTNER HAFTBAR GEMACHT WERDEN/WIRD, DIE HAFTUNG DES RECHTSINHABERS UND/ODER SEINER PARTNER AUF DIE KOSTEN DER SOFTWARE BESCHRÄNKT IST. UNTER KEINEN UMSTÄNDEN WIRD DIE HAFTUNG DES RECHTSINHABERS UND/ODER SEINER PARTNER DIE FÜR DIE SOFTWARE ERSTATTETEN KOSTEN AN DEN RECHTSINHABER ODER DEN PARTNER ÜBERSTEIGEN (JE NACHDEM, WAS ZUTRIFFT).

NICHTS IN DIESEM VERTRAG SCHLIEßT EINEN ANSPRUCH AUFGRUND VON TOD UND PERSONENSCHADEN AUS ODER SCHRÄNKT DIESEN EIN. IN DEM FALL, DASS EIN HAFTUNGSAUSSCHLUSS, EIN AUSSCHLUSS ODER EINE EINSCHRÄNKUNG IN DIESEM VERTRAG AUFGRUND GELTENDEN RECHTS NICHT AUSGESCHLOSSEN ODER BESCHRÄNKT WERDEN KANN, WIRD NUR EIN SOLCHER HAFTUNGSAUSSCHLUSS, AUSSCHLUSS ODER EINE EINSCHRÄNKUNG NICHT FÜR SIE GELTEN, UND SIE SIND WEITERHIN AN JEDWEDE VERBLEIBENDEN HAFTUNGSAUSSCHLÜSSE, AUSSCHLÜSSE ODER EINSCHRÄNKUNGEN GEBUNDEN.

8. GNU und sonstige Drittpartei-Lizenzen

Die Software kann einige Softwareprogramme enthalten, die an den Nutzer unter der GPL (GNU General Public License) oder sonstigen vergleichbaren freien Softwarelizenzen lizenziert (oder unterlizenziert) sind und dem Nutzer neben anderen Rechten gestatten, bestimmte Programme oder Teile dieser Programme zu kopieren, zu modifizieren und weiter zu verbreiten und sich Zugang zum Quellcode zu verschaffen („Open Source Software“). Falls es solche Lizenzen erforderlich machen, dass für jedwede Software, die an jemanden in ausführbarem Binärformat geliefert wird, diesen Nutzern der Quellcode ebenfalls verfügbar gemacht wird, dann soll der Quellcode zur Verfügung gestellt werden, indem ein diesbezügliches Ersuchen an source@kaspersky.com gesendet wird, oder der Quellcode wird mit der Software geliefert. Falls irgendwelche Open Source Software-Lizenzen es erforderlich machen, dass der Rechtsinhaber Rechte zur Nutzung, zum Kopieren oder zur Änderung eines Open Source Software-Programms bereitstellt, welche umfassender sind, als die in diesem Vertrag gewährten Rechte, dann werden derartige Rechte Vorrang vor den hierin festgelegten Rechten und Einschränkungen haben.

9. Geistiges Eigentum

9.1 Sie stimmen zu, dass die Software sowie die Urheberschaft, Systeme, Ideen, Betriebsmethoden, Dokumentation und sonstige in der Software enthaltenen Informationen proprietäres geistiges Eigentum und/oder die wertvollen Geschäftsgeheimnisse des Rechtsinhabers oder seiner Partner sind und dass der Rechtsinhaber und seine Partner, je nachdem was zutrifft, durch das Zivil- und Strafrecht sowie durch Gesetze

zum Urheberrecht, bezüglich Geschäftsgeheimnissen, Handelsmarken und Patenten der Russischen Föderation, der Europäischen Union und der Vereinigten Staaten sowie anderer Länder und internationaler Übereinkommen geschützt sind. Dieser Vertrag gewährt Ihnen keinerlei Rechte am geistigen Eigentum, einschließlich an jeglichen Handelsmarken und Servicemarken des Rechtsinhabers und/oder seiner Partner („Handelsmarken"). Sie dürfen die Handelsmarken nur so weit nutzen, um von der Software im Einklang mit der akzeptierten Handelsmarkenpraxis erstellte Druckausgaben zu identifizieren, einschließlich der Identifizierung des Namens des Besitzers der Handelsmarke. Eine solche Nutzung der Handelsmarke gibt Ihnen keinerlei Besitzrechte an dieser Handelsmarke. Der Rechtsinhaber und/oder seine Partner besitzen und behalten alle Rechte, Titel und Anteile an der Software, einschließlich (ohne jedwede Einschränkung) jedweden Fehlerkorrekturen, Erweiterungen, Updates oder sonstigen Modifikationen an der Software, ob durch den Rechtsinhaber oder eine beliebige Drittpartei vorgenommen, und allen Urheberrechten, Patenten, Rechten an Geschäftsgeheimnissen, Handelsmarken und sonstigem geistigen Eigentum daran. Ihr Besitz, die Installation oder Nutzung der Software lässt den Titel am geistigen Eigentum an der Software nicht auf Sie übergehen, und Sie erwerben keinerlei Rechte an der Software, außer jene ausdrücklich in diesem Vertrag dargelegten. Alle hierunter erstellten Kopien der Software müssen dieselben proprietären Informationen enthalten, die auf und in der Software erscheinen. Mit Ausnahme der hierin aufgeführten Bestimmungen gewährt Ihnen dieser Vertrag keine Rechte geistigen Eigentums an der Software und Sie bestätigen, dass diese unter diesem Vertrag gewährte Lizenz Ihnen gemäß den weiteren Festlegungen hierin ausschließlich das Recht auf eingeschränkte Nutzung unter den Geschäftsbedingungen dieses Vertrags gewährt. Der Rechtsinhaber behält sich alle Rechte vor, die Ihnen nicht ausdrücklich in diesem Vertrag gewährt wurden.

9.2 Sie bestätigen, dass der Quellcode, der Aktivierungscode und/oder die Lizenzschlüssel-Datei für die Software Eigentum des Rechtsinhabers sind und Geschäftsgeheimnisse des Rechtsinhabers konstituieren. Sie stimmen zu, den Quellcode der Software nicht zu modifizieren, abzuwandeln, zu übersetzen, zurückzuentwickeln, zu dekompilieren oder auf sonstige Weise zu versuchen, den Quellcode ausfindig zu machen.

9.3 Sie stimmen zu, die Software in keinster Weise zu modifizieren oder abzuändern. Sie dürfen die Urheberrechtshinweise oder sonstige proprietäre Hinweise auf jedweden Kopien der Software nicht entfernen oder verändern.

10. Geltendes Recht; Schiedsverfahren

Dieser Vertrag unterliegt den Gesetzen der Russischen Föderation und wird nach diesen ausgelegt, und zwar ohne Bezug auf gegenteilige gesetzliche Regelungen und Prinzipien. Dieser Vertrag wird nicht dem Übereinkommen der Vereinten Nationen über Verträge über den internationalen Warenverkauf unterliegen, dessen Anwendung ausschließlich ausgeschlossen wird. Jede Meinungsverschiedenheit, die aus den Bedingungen dieses Vertrags, deren Auslegung oder Anwendung oder einem Verstoß gegen diese resultiert, wird, außer falls durch unmittelbare Verhandlung beigelegt, durch das Gericht der internationalen Handelsschiedsgerichtsbarkeit bei der Industrie- und Handelskammer der Russischen Föderation in Moskau, in der Russischen Föderation, beigelegt. Jeder vom Schlichter abgegebene Schiedsspruch ist für die beteiligten Parteien endgültig und bindend und jedwedes Urteil bezüglich eines solchen Schiedsspruchs kann von jedem Gericht der zuständigen Jurisdiktion durchgesetzt werden. Nichts in diesem Abschnitt 10 wird eine Partei daran hindern, von einem Gericht der zuständigen Jurisdiktion rechtmäßige Entschädigung zu verlangen oder zu erhalten, sei es vor, während oder nach einem Schiedsverfahren.

11. Zeitraum für Rechtsverfolgung.

Von den Parteien dieses Vertrags kann keine Rechtsverfolgung, ungeachtet der Form, die sich aus Transaktionen unter diesem Vertrag ergibt, nach mehr als einem (1) Jahr nach dem Eintreten des Klagegrundes oder der Entdeckung dessen Eintritts ergriffen werden, außer, dass eine Rechtsverfolgung für Verletzung von Rechten geistigen Eigentums innerhalb des maximal geltenden gesetzlichen Zeitraums ergriffen wird.

12. Vollständigkeit der Vereinbarung, Salvatorische Klausel, kein Verzicht.

Dieser Vertrag stellt die Gesamtvereinbarung zwischen Ihnen und dem Rechtsinhaber dar und ersetzt jegliche sonstigen, vorherigen Vereinbarungen, Vorschläge, Kommunikation oder Ankündigung, ob mündlich oder schriftlich, in Bezug auf die Software oder den Gegenstand dieser Vereinbarung. Sie bestätigen, dass Sie diesen Vertrag gelesen haben, ihn verstehen und seinen Bedingungen zustimmen. Falls eine Bestimmung dieses Vertrags von einem Gericht der zuständigen Jurisdiktion insgesamt oder in Teilen als untauglich, ungültig oder aus welchen Gründen auch immer als nicht durchsetzbar angesehen wird, wird diese Bestimmung enger ausgelegt, damit sie rechtmäßig und durchsetzbar wird, und der Gesamtvertrag wird an diesem Umstand nicht scheitern, und die Ausgewogenheit des Vertrags bleibt weiterhin vollinhaltlich gültig und wirksam, so weit gesetzlich oder nach Billigkeitsrecht zulässig, während der ursprüngliche Inhalt weitest möglich beibehalten wird. Kein Verzicht auf eine hierin enthaltene Bestimmung oder Kondition ist gültig, außer in schriftlicher Form und durch Sie und einen autorisierten Vertreter des Rechtsinhabers unterzeichnet, vorausgesetzt, dass kein Verzicht einer Verletzung einer Bestimmung dieses Vertrags einen Verzicht eines vorherigen, gleichzeitigen oder Folgeverstoßes konstituiert. Nichtverfolgung oder fehlende Durchsetzung einer

Bestimmung dieses Vertrags durch den Rechtsinhaber kann nicht als Verzicht auf diese Bestimmung oder dieses Recht geltend gemacht werden.

13. Kontaktinformationen des Rechteinhabers.

Sollten Sie Fragen in Bezug auf diesen Vertrag haben oder sollten Sie wünschen, sich aus irgendeinem Grund mit dem Rechtsinhaber in Verbindung zu setzen, kontaktieren Sie bitte unsere Kundendienstabteilung unter:

Kaspersky Lab ZAO, 10 build. 1, 1st Volokolamsky Proezd
Moskau, 123060
Russische Föderation
Tel.: +7-495-797-8700
Fax: +7-495-645-7939
E-Mail: info@kaspersky.com
Webseite: www.kaspersky.com

© 1997-2010 Kaspersky Lab ZAO. Alle Rechte vorbehalten. Die Software und jedwede begleitende Dokumentation unterliegen dem Urheberrecht bzw. dem Schutz durch Urheberrechtsgesetze und internationale Urheberrechtsabkommen sowie durch weitere Gesetze und Abkommen zum geistigen Eigentum.

INHALT

ENDNUTZER-LIZENZVERTRAG FÜR KASPERSKY LAB SOFTWARE 3

KASPERSKY MOBILE SECURITY 9.0 14

Suche nach Informationen über das Programm 15

Informationsquellen zur selbständigen Recherche 15

Kontaktaufnahme mit der Vertriebsabteilung 16

Diskussion über die Programme von Kaspersky Lab im Webforum 16

Neuerungen in Kaspersky Mobile Security 9.0 16

Hard- und Softwarevoraussetzungen 17

Lieferumfang 17

KASPERSKY MOBILE SECURITY 9.0 FÜR SYMBIAN OS 18

Kaspersky Mobile Security 9.0 installieren 18

Programm deinstallieren 19

Upgrade von Programmversion 8.0 auf Version 9.0 22

Erste Schritte 23

Programm aktivieren 23

Geheimcode eingeben 27

Programm starten 28

Update der Programm-Datenbanken 28

Gerät auf Viren untersuchen 29

Programm-Info anzeigen 29

Lizenzverwaltung 29

Über den Lizenzvertrag 30

Über Lizenzen für Kaspersky Mobile Security 30

Über Schlüsseldateien für Kaspersky Mobile Security 30

Lizenz-Info anzeigen 31

Lizenz verlängern 32

Programmoberfläche 34

Schutzsymbol 34

Fenster für den Schutzstatus 34

Registerkarten des Programms 36

Programm-Menü 37

Schutz für das Dateisystem 37

Schutz 38

Schutz aktivieren / deaktivieren 38

Schutzbereich anpassen 39

Aktion für gefundene Objekte wählen 40

Standardmässige Schutzeinstellungen wiederherstellen 41

Untersuchung des Geräts 41

Über die Untersuchung des Geräts 42

Untersuchung manuell starten 42

Untersuchung nach Zeitplan starten 44

Typ der Untersuchungsobjekte wählen 45

Aktion für gefundene Objekte wählen 46

Archiv-Untersuchung anpassen 48

Standardmässige Einstellungen für die Untersuchung des Geräts wiederherstellen 49

Quarantäne für möglicherweise infizierte Objekte ... 49
Quarantäne ... 50
Quarantäneobjekte anzeigen ... 50
Quarantäneobjekte wiederherstellen ... 51
Quarantäneobjekte löschen ... 51
Eingehende Anrufe und SMS-Nachrichten filtern ... 51
Anti-Spam ... 52
Über die Modi für Anti-Spam ... 53
Anti-Spam-Modus ändern ... 53
Schwarze Liste anlegen ... 54
Weisse Liste anlegen ... 57
Reaktion auf SMS-Nachrichten und Anrufe von Kontakten, die nicht im Telefonbuch stehen ... 60
Reaktion auf SMS-Nachrichten von Nicht-Ziffern-Nummern ... 61
Aktion für eingehende SMS-Nachrichten wählen ... 62
Aktion für eingehende Anrufe wählen ... 63
Ausgehende Anrufe und SMS-Nachrichten einschränken ... 64
Kindersicherung ... 64
Modi der Kindersicherung ... 65
Modus für die Kindersicherung ändern ... 65
Schwarze Liste anlegen ... 66
Weisse Liste anlegen ... 69
Datenschutz bei Verlust oder Diebstahl des Geräts ... 72
Diebstahlschutz ... 73
Gerät blockieren ... 73
Persönliche Daten löschen ... 75
Liste der zu löschenden Objekte erstellen ... 77
Wechsel der SIM-Karte auf dem Gerät überwachen ... 78
Geografische Koordinaten des Geräts ermitteln ... 79
Diebstahlschutz-Funktionen ferngesteuert starten ... 81
Private Daten verbergen ... 82
Über die Privatsphäre ... 83
Über die Modi der Privatsphäre ... 83
Privatsphären-Modus ändern ... 83
Privatsphäre automatisch starten ... 84
Privatsphäre ferngesteuert starten ... 85
Liste der geschützten Kontakte erstellen ... 87
Schutzobjekte wählen: Privatsphäre ... 89
Netzwerkaktivität filtern ... 90
Firewall ... 91
Über die Sicherheitsstufen der Firewall ... 91
Sicherheitsstufe der Firewall wählen ... 91
Meldung über Verbindungsversuch ... 92
Persönliche Daten verschlüsseln ... 93
Verschlüsselung ... 93
Daten verschlüsseln ... 94
Daten entschlüsseln ... 95
Zugriff auf verschlüsselte Daten verbieten ... 96
Update der Programm-Datenbanken ... 97
Über das Update der Programm-Datenbanken ... 98

Datenbankinfos anzeigen ... 98
Update manuell starten ... 99
Update nach Zeitplan starten ... 100
Update im Roaming ... 101
Einstellungen der Internetverbindung anpassen ... 102
Programmberichte ... 103
Berichte ... 103
Berichtseinträge anzeigen ... 103
Berichtseinträge löschen ... 104
Erweiterte Einstellungen anpassen ... 104
Geheimcode ändern ... 105
Tooltips anzeigen ... 105
Audiosignale verwalten ... 105
Hintergrundbeleuchtung verwalten ... 106
Statusfenster anzeigen ... 107
Schutzsymbol anzeigen ... 108
KASPERSKY MOBILE SECURITY 9.0 FÜR MICROSOFT WINDOWS MOBILE ... 110
Kaspersky Mobile Security 9.0 installieren ... 110
Programm deinstallieren ... 111
Upgrade von Programmversion 8.0 auf Version 9.0 ... 113
Erste Schritte ... 114
Programm aktivieren ... 114
Geheimcode eingeben ... 117
Programm starten ... 118
Update der Programm-Datenbanken ... 118
Gerät auf Viren untersuchen ... 118
Programm-Info anzeigen ... 119
Lizenzverwaltung ... 119
Programmoberfläche ... 124
Fenster für den Schutzstatus ... 124
Programm-Menü ... 126
Schutz für das Dateisystem ... 127
Schutz ... 127
Schutz aktivieren / deaktivieren ... 128
Aktion für gefundene Objekte wählen ... 129
Untersuchung des Geräts ... 130
Über Scan auf Befehl ... 131
Untersuchung manuell starten ... 131
Untersuchung nach Zeitplan starten ... 133
Typ der Untersuchungsobjekte wählen ... 134
Archiv-Untersuchung anpassen ... 135
Aktion für gefundene Objekte wählen ... 136
Quarantäne für schädliche Objekte ... 137
Quarantäne ... 137
Quarantäneobjekte anzeigen ... 138
Quarantäneobjekte wiederherstellen ... 138
Quarantäneobjekte löschen ... 139
Eingehende Anrufe und SMS-Nachrichten filtern ... 139

Anti-Spam ... 140
Über die Modi für Anti-Spam ... 141
Anti-Spam-Modus ändern ... 141
Schwarze Liste anlegen ... 142
Weisse Liste anlegen ... 145
Reaktion auf SMS-Nachrichten und Anrufe von Kontakten, die nicht im Telefonbuch stehen ... 148
Reaktion auf SMS-Nachrichten von Nicht-Ziffern-Nummern ... 149
Aktion für eingehende SMS-Nachrichten wählen ... 150
Aktion für eingehende Anrufe wählen ... 151
Ausgehende Anrufe und SMS-Nachrichten einschränken ... 152
Kindersicherung ... 153
Modi der Kindersicherung ... 153
Kindersicherung aktivieren / deaktivieren ... 153
Schwarze Liste anlegen ... 154
Weisse Liste anlegen ... 157
Datenschutz bei Verlust oder Diebstahl des Geräts ... 160
Diebstahlschutz ... 161
Gerät blockieren ... 162
Persönliche Daten löschen ... 163
Liste der zu löschenden Daten erstellen ... 166
Wechsel der SIM-Karte auf dem Gerät überwachen ... 167
Geografische Koordinaten des Geräts ermitteln ... 168
Diebstahlschutz-Funktionen ferngesteuert starten ... 170
Persönliche Daten verbergen ... 171
Über die Privatsphäre ... 172
Über die Modi der Privatsphäre ... 172
Privatsphäre aktivieren / deaktivieren ... 172
Privatsphäre automatisch starten ... 173
Privatsphäre ferngesteuert starten ... 174
Liste der geschützten Kontakte erstellen ... 176
Schutzobjekte wählen: Privatsphäre ... 178
Netzwerkaktivität filtern ... 180
Firewall ... 180
Firewall aktivieren / deaktivieren ... 180
Sicherheitsstufe der Firewall wählen ... 180
Persönliche Daten verschlüsseln ... 181
Verschlüsselung ... 181
Daten verschlüsseln ... 182
Daten entschlüsseln ... 183
Zugriff auf verschlüsselte Daten verbieten ... 185
Update der Programm-Datenbanken ... 186
Über das Update der Programm-Datenbanken ... 186
Datenbank-infos anzeigen ... 187
Manuelles Update ... 188
Update nach Zeitplan ... 189
Update im Roaming ... 190
Programmberichte ... 191
Berichte ... 191
Berichtseinträge anzeigen ... 191

Einträge aus Bericht löschen 192
Erweiterte Einstellungen anpassen 193
Geheimcode ändern 193
Tooltips anzeigen 194
Audiosignale verwalten 195
KONTAKTAUFNAHME MIT DEM TECHNISCHEN SUPPORT 196
GLOSSAR 197
KASPERSKY LAB 200
CRYPTOEX OOO 201
SACHREGISTER 202

KASPERSKY MOBILE SECURITY 9.0

Kaspersky Mobile Security 9.0 schützt mobile Geräte, die mit den Betriebssystemen Symbian OS und Microsoft Windows Mobile arbeiten, vor bekannten und neuen Gefahren, unerwünschten Anrufen und SMS-Nachrichten. Das Programm kontrolliert ausgehende SMS-Nachrichten und die Netzwerkaktivität. Außerdem schützt es vertrauliche Daten vor unbefugtem Zugriff. Jeder Bedrohungstyp wird von bestimmten Programmkomponenten verarbeitet. Dadurch wird erlaubt, die Programmeinstellungen flexibel an die Erfordernisse eines konkreten Benutzers anzupassen.

Kaspersky Mobile Security 9.0 umfasst folgende Schutzkomponenten:

- **Schutz**. Schützt das Dateisystem des mobilen Geräts vor Infektionen. Die Komponente *Schutz* wird beim Hochfahren des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Geräts und untersucht alle Dateien, die auf dem Gerät und auf Speicherkarten geöffnet, gespeichert und gestartet werden. Außerdem untersucht der Schutz alle eingehenden Dateien auf bekannte Viren. Eine Datei wird nur dann zur Arbeit freigegeben, wenn das Objekt virenfrei ist oder erfolgreich desinfiziert wurde.

- **Untersuchung des Geräts**. Hilft dabei, schädliche Objekte auf Ihrem Gerät zu erkennen und zu neutralisieren. Das Gerät sollte regelmäßig untersucht werden, um die Ausbreitung schädlicher Objekte zu verhindern, die vom Schutz nicht gefunden wurden.

- **Anti-Spam**. Prüft alle eingehenden SMS-Nachrichten und Anrufe auf Spam. Die Komponente blockiert alle SMS-Nachrichten und Anrufe, die als unerwünscht gelten.

- **Kindersicherung**. Kontrolliert alle ausgehenden Nachrichten und Anrufe und verbietet ausgehende SMS-Nachrichten und / oder Anrufe an zuvor festgelegte Nummern.

- **Diebstahlschutz**. Schützt die Informationen auf dem Gerät vor unbefugtem Zugriff, wenn das Gerät verloren geht oder gestohlen wird. Die Komponente kann das Gerät bei Verlust oder Diebstahl ferngesteuert blockieren, vertrauliche Informationen löschen, einen Wechsel der SIM-Karte kontrollieren und das Gerät orten (falls das Gerät einen GPS-Empfänger besitzt).

- **Privatsphäre**. Verbirgt sensible Informationen des Benutzers, wenn das Gerät von anderen Personen verwendet wird. Die Komponente kann alle Informationen, die mit festgelegten Nummern zusammenhängen, anzeigen oder verbergen. Zu diesen Daten gehören z.B. Daten der Kontaktliste, SMS-Nachrichten und Einträge der Anrufliste. Außerdem kann diese Komponente die Anrufe und SMS-Nachrichten, die von festgelegten Nummern eingehen, verbergen.

- **Firewall**. Kontrolliert die Netzwerkverbindungen auf Ihrem mobilen Gerät. Mit dieser Komponente können Verbindungen festgelegt werden, die erlaubt und blockiert werden sollen.

- **Verschlüsselung**. Schützt die Informationen auch dann vor dem Zugriff durch Dritte, wenn das Gerät in fremde Hände geraten sollte. Die Komponente verschlüsselt eine beliebige Anzahl von Ordnern. Die Ordner können sich im Speicher des Geräts oder auf Speicherkarten befinden. Die Daten eines Ordners sind nur nach Eingabe des Geheimcodes verfügbar.

Das Programm verfügt außerdem über eine Reihe von Servicefunktionen. Sie halten das Programm auf dem neuesten Stand, erweitern die Einsatzmöglichkeiten des Programms und unterstützen den Benutzer bei der Arbeit.

- Update der Programm-Datenbanken. Diese Funktion hält die Datenbanken von Kaspersky Mobile Security 9.0 aktuell.

- Schutzstatus. Auf dem Display werden die Status der Programmkomponenten angezeigt. Auf Basis der angezeigten Informationen können Sie den aktuellen Schutzstatus Ihres Geräts einschätzen.

- Ereignisbericht. Das Programm führt für jede Komponente einen separaten Ereignisbericht, der die Arbeit der Komponente dokumentiert (z.B. ausgeführte Operation, Daten über ein blockiertes Objekt, Untersuchungs- oder Updatebericht, u.a.).

- Lizenz. Beim Kauf von Kaspersky Mobile Security 9.0 wird zwischen Ihnen und Kaspersky Lab ein Lizenzvertrag abgeschlossen, der die Bedingungen für die Nutzung des Programms und den Zugriff auf Updates der

Programm-Datenbanken und auf den technischen Support festlegt. Die Nutzungsdauer und sonstige Informationen, die für die volle Funktionsfähigkeit des Programms erforderlich sind, sind in der Lizenz enthalten.

Mit der Funktion **Lizenz** können Sie sich ausführlich über die von Ihnen verwendete Lizenz informieren und deren Gültigkeit verlängern.

Kaspersky Mobile Security 9.0 führt keine Datensicherung und Datenwiederherstellung aus.

IN DIESEM ABSCHNITT

Suche nach Informationen über das Programm 15

Neuerungen in Kaspersky Mobile Security 9.0 16

Hard- und Softwarevoraussetzungen 17

Lieferumfang 17

SUCHE NACH INFORMATIONEN ÜBER DAS PROGRAMM

Wenn Sie Fragen zu Auswahl, Kauf, Installation oder Verwendung von Kaspersky Mobile Security haben, können Sie schnell eine Antwort darauf erhalten.

Kaspersky Lab bietet unterschiedliche Informationsquellen zu dem Programm an. Abhängig von Dringlichkeit und Bedeutung Ihrer Frage können Sie unter diesen Quellen wählen.

IN DIESEM ABSCHNITT

Informationsquellen zur selbständigen Recherche..... 15

Kontaktaufnahme mit der Vertriebsabteilung..... 16

Diskussion über die Programme von Kaspersky Lab im Webforum..... 16

INFORMATIONSQUELLEN ZUR SELBSTÄNDIGEN RECHERCHE

Bei Fragen über die Anwendung stehen folgende Informationsquellen zur Verfügung:

- Webseite von Kaspersky Lab
- Webseite des technischen Supports (in der Wissensdatenbank)
- elektronisches Hilfesystem und Tooltips
- Dokumentationen

Webseite von Kaspersky Lab

www.kaspersky.de/mobile_security

Auf dieser Seite finden Sie allgemeine Informationen über Kaspersky Mobile Security, seine Funktionen und Besonderheiten. Außerdem können Sie in unserem Online-Shop Kaspersky Mobile Security kaufen.

Webseite des technischen Supports (Wissensdatenbank)

http://support.kaspersky.com/de/

Auf dieser Seite finden Sie Artikel, die von Spezialisten des technischen Supports veröffentlicht wurden.

Diese Artikel bieten nützliche Informationen, Tipps und Antworten auf häufige Fragen zu Kauf, Installation und Verwendung von Kaspersky Mobile Security. Sie sind nach Themen wie "Arbeit mit Schlüsseldateien", "Datenbank-Update" oder "Beheben von Störungen bei der Arbeit" angeordnet. Die Artikel können auch Fragen behandeln, die neben Kaspersky Mobile Security auch andere Produkte von Kaspersky Lab betreffen. Außerdem können Sie Neuigkeiten über den technischen Support enthalten.

Elektronisches Hilfesystem

Bei Fragen zu einem speziellen Fenster oder zu einer Registerkarte von Kaspersky Mobile Security hilft Ihnen die Kontexthilfe.

Um die Kontexthilfe zu öffnen, öffnen Sie die Sie interessierende Registerkarte des Fensters und gehen Sie auf den Punkt **Hilfe**.

Dokumentation

Das Benutzerhandbuch informiert ausführlich über die Programmfunktionen und erläutert unterschiedliche Konfigurationen.

Das Benutzerhandbuch ist als PDF im Lieferumfang von Kaspersky Mobile Security enthalten.

Außerdem stehen die Dokumente auf der Webseite von Kaspersky Lab zum Download bereit.

KONTAKTAUFNAHME MIT DER VERTRIEBSABTEILUNG

Bei Fragen zur Auswahl oder zum Kauf von Kaspersky-Produkten sowie zur Verlängerung der Nutzungsdauer stehen Ihnen die Mitarbeiter der Vertriebsabteilung in Deutschland unter folgenden Rufnummern zur Verfügung:

+49 (0) 841 – 981 89 560

Die Beratung erfolgt auf Deutsch oder Englisch.

Sie können sich mit Ihrer Frage auch über unser Kontaktformular an die Mitarbeiter der Vertriebsabteilung wenden.

DISKUSSION ÜBER DIE PROGRAMME VON KASPERSKY LAB IM WEBFORUM

Wenn Ihre Frage nicht dringend ist, können Sie sie mit den Spezialisten von Kaspersky Lab und mit anderen Anwendern in unserem Forum unter der Adresse http://forum.kaspersky.com diskutieren.

Im Forum können Sie bereits veröffentlichte Themen nachlesen, eigene Beiträge schreiben, neue Themen eröffnen und die Hilfefunktion verwenden.

NEUERUNGEN IN KASPERSKY MOBILE SECURITY 9.0

Ausführliche Beschreibung der Neuerungen in Kaspersky Mobile Security 9.0.

Neuerungen im Schutz:

- Der Zugriff auf das Programm wird durch einen Geheimcode geschützt.

- Kaspersky Mobile Security 9.0 verfügt über die neue Komponente *Privatsphäre*. Sie verhindert den unbefugten Zugriff auf persönliche Benutzerdaten, wenn das Gerät vorübergehend von Dritten verwendet wird. Die Komponente verbirgt Daten und Ereignisse, die bestimmte Nummern betreffen. Die Aktivität der Komponente *Privatsphäre* bleibt unbemerkt. Es gibt keine Hinweise darauf, dass auf dem Gerät verborgene Daten vorhanden sind.

- Das überarbeitete Verschlüsselungsmodul erlaubt es, den Zugriff auf eine beliebige Anzahl von Ordnern, die sich im Speicher des Geräts oder auf einer Speicherkarte befinden, zu sperren. Die Komponente speichert vertrauliche Daten in verschlüsselter Form und blockiert nach einer festgelegten Dauer automatisch den Zugriff.

- Im Programm wurde eine neue Methode zur Verwaltung des Geräteschutzes realisiert: Der Benutzer kann situationsabhängig jede Komponente separat aktivieren und deaktivieren.

- Der Kauf eines Aktivierungscodes und eine Lizenzverlängerung sind nun im Online-Modus direkt vom mobilen Gerät aus möglich.

HARD- UND SOFTWAREVORAUSSETZUNGEN

Kaspersky Mobile Security 9.0 kann auf mobilen Geräten installiert werden, die mit den folgenden Betriebssystemen arbeiten:

- Symbian OS 9.1, 9.2, 9.3 und 9.4 Series 60 UI

- Microsoft Windows Mobile 5.0, 6.0, 6.1, 6.5.

LIEFERUMFANG

Kaspersky Mobile Security kann über das Internet bezogen werden (Programm und Dokumentation in elektronischer Form). Außerdem wird Kaspersky Mobile Security über den Fachhandel vertrieben.

KASPERSKY MOBILE SECURITY 9.0 FÜR SYMBIAN OS

In diesem Abschnitt wird die Funktionsweise von Kaspersky Mobile Security 9.0 für mobile Geräte beschrieben, die mit dem Betriebssystem Symbian 9.1, 9.2, 9.3 oder 9.4 Series 60 UI arbeiten.

IN DIESEM ABSCHNITT

Kaspersky Mobile Security 9.0 installieren 18

Programm deinstallieren 19

Upgrade von Programmversion 8.0 auf Version 9.0 22

Erste Schritte 23

Lizenzverwaltung 29

Programmoberfläche 34

Schutz für das Dateisystem 37

Untersuchung des Geräts 41

Quarantäne für möglicherweise infizierte Objekte 49

Eingehende Anrufe und SMS-Nachrichten filtern 51

Ausgehende Anrufe und SMS-Nachrichten einschränken. Kindersicherung 64

Datenschutz bei Verlust oder Diebstahl des Geräts 72

Private Daten verbergen 82

Netzwerkaktivität filtern. Firewall 90

Persönliche Daten verschlüsseln 93

Update der Programm-Datenbanken 97

Programmberichte 103

Erweiterte Einstellungen anpassen 104

KASPERSKY MOBILE SECURITY 9.0 INSTALLIEREN

Die Installation des Programms auf einem mobilen Gerät umfasst mehrere Schritte.

Zur Installation von Kaspersky Mobile Security 9.0:

1. Schließen Sie das mobile Gerät an einen Computer an.

   Für Smartphones des Herstellers Nokia wird empfohlen, das Programm Nokia PC Suite zu verwenden.

2. Führen Sie eine der folgende Aktionen aus:

   - Wenn Sie das Programm auf CD erworben haben, starten Sie auf der CD die automatische Installation von Kaspersky Mobile Security 9.0.
   - Wenn Sie die Installationsdatei über das Internet bezogen haben, kopieren Sie sie auf das mobile Gerät. Dazu stehen folgende Methoden zur Verfügung:
     - mit dem Programm Nokia PC Suite (für Smartphones der Firma Nokia)
     - mit einer Speicherkarte

     Starten Sie danach die Installation mit einer der folgenden Varianten:

     - aus dem Programm Nokia PC Suite (für mobile Geräte der Firma Nokia)
     - indem Sie das sis-Archiv der Distribution auf dem mobilen Gerät öffnen

   Es wird ein Fenster zur Bestätigung der Installation geöffnet.

3. Bestätigen Sie die Installation des Programms mit **Ja**.

4. Prüfen Sie Name, Version und Zertifikate des Programms. Klicken Sie dann auf **Weiter**.

   Wenn die Sprache des Betriebssystems nicht mit der Sprache von Kaspersky Mobile Security 9.0 übereinstimmt, erscheint eine Meldung auf dem Bildschirm. Klicken Sie auf **OK**, um mit der Installation des Programms in der aktuellen Sprache fortzufahren.

5. Lesen Sie den Lizenzvertrag, der zwischen Ihnen und Kaspersky Lab abgeschlossen wird. Klicken Sie auf **OK**, wenn Sie die Vertragsbedingungen akzeptieren. Danach wird Kaspersky Mobile Security 9.0 auf dem Gerät installiert. Klicken Sie auf **Abbrechen**, wenn Sie den Bedingungen des Lizenzvertrags nicht zustimmen. Die Installation wird in diesem Fall abgebrochen.

6. Bestätigen Sie mit **OK**, dass auf dem mobilen Gerät keine anderen Antiviren-Programme installiert sind.

7. Starten Sie das Gerät neu, um die Installation abzuschließen.

   Das Programm wird mit den von Kaspersky Lab empfohlenen Einstellungen installiert.

PROGRAMM DEINSTALLIEREN

Gehen Sie folgendermaßen vor, um Kaspersky Mobile Security 9.0 zu löschen.

1. Wenn auf Ihrem Gerät Daten vorhanden sind, die mit Kaspersky Mobile Security 9.0 verschlüsselt wurden, entschlüsseln Sie die Daten (s. Abschnitt "Daten entschlüsseln" auf S. 95).

2. Deaktivieren Sie die Privatsphäre (s. Abschnitt "Über die Modi der Privatsphäre" auf S. 83).

3. Beenden Sie Kaspersky Mobile Security 9.0. Gehen Sie dazu auf **Optionen** → **Beenden** (s. Abb. unten).

Abbildung 1. Programm beenden

4. Entfernen Sie Kaspersky Mobile Security 9.0. Gehen Sie dazu folgendermaßen vor:

   a. Öffnen Sie das Hauptmenü des Geräts.

   b. Wählen Sie **Programme** → **Persönlich** (s. Abb. unten).

Der Installationsordner für das Programm kann je nach Modell des mobilen Geräts variieren.

Abbildung 2. Programm-Manager starten

c. Wählen Sie in der Programmliste **KMS 9.0** und gehen Sie dann auf **Optionen** → **Entfernen** (s. Abb. unten).

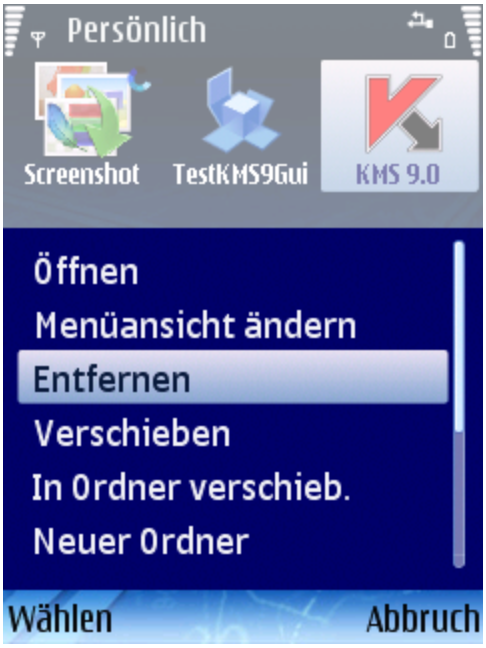


Abbildung 3. Programm deinstallieren

d. Bestätigen Sie die Deinstallation des Programms mit **Ja**.

e. Geben Sie den Geheimcode ein und klicken Sie auf **OK**.

f. Legen Sie fest, ob Programmeinstellungen und Quarantäneobjekte gespeichert werden sollen:

- Wenn Sie Programmeinstellungen und Quarantäneobjekte beibehalten möchten, aktivieren Sie die entsprechenden Kontrollkästchen und klicken Sie auf **OK** (s. Abb. unten).
- Klicken Sie auf **Abbrechen**, um das Programm vollständig zu deinstallieren.

Abbildung 4. Zu speichernde Einstellungen wählen

5. Starten Sie das Gerät neu, um die Deinstallation des Programms abzuschließen.

UPGRADE VON PROGRAMMVERSION 8.0 AUF VERSION 9.0

Wenn auf Ihrem Gerät bereits Kaspersky Mobile Security 8.0 installiert ist, können Sie es auf Kaspersky Mobile Security 9.0 aktualisieren.

Bevor Sie das Programm auf eine andere Version upgraden, deaktivieren Sie die Verschlüsselung und entschlüsseln Sie alle Daten (s. Abschnitt "Daten entschlüsseln" auf S. 95).

Gehen Sie folgendermaßen vor, um das Programm auf die neue Version zu aktualisieren:

1. Beenden Sie die aktuelle Version von Kaspersky Mobile Security. Gehen Sie dazu auf **Optionen** → **Beenden**.
2. Kopieren Sie die Installationsdatei auf das mobile Gerät. Dazu stehen folgende Methoden zur Verfügung:
   - von der Webseite von Kaspersky Lab
   - mit dem Programm Nokia PC Suite (für Smartphones der Firma Nokia)
   - mit einer Speicherkarte
3. Starten Sie auf dem Gerät das Setup für Kaspersky Mobile Security 9.0.
4. Bestätigen Sie die Installation des Programms mit **Ja**.
5. Prüfen Sie Name, Version und Zertifikate des Programms. Klicken Sie dann auf **Fortfahren**.
6. Bestätigen Sie das Programm-Upgrade mit **OK**.
7. Geben Sie den Geheimcode aus der Vorgängerversion des Programms ein.
8. Lesen Sie den Lizenzvertrag genau. Wenn Sie den Vertragsbestimmungen zustimmen, klicken Sie auf **OK**. Klicken Sie auf **Abbruch**, wenn Sie den Bedingungen des Lizenzvertrags nicht zustimmen. Die Installation wird in diesem Fall abgebrochen.
9. Bestätigen Sie, dass auf dem mobilen Gerät keine anderen Antiviren-Programme installiert sind. Klicken Sie dazu auf **OK**.
10. Löschen Sie die Einstellungen, die in der vorherigen Programmversion verwendet wurden. Klicken Sie dazu auf **Löschen**.

    Die Einstellungen können nur gespeichert werden, wenn ein Wechsel zwischen Versionen der gleichen Produktgeneration erfolgt. Die Programmeinstellungen von 8.0 sind nicht mit Programmversion 9.0 kompatibel.

    Die Installation von Kaspersky Mobile Security 9.0 beginnt.

    Wenn die Lizenz für Kaspersky Mobile Security 8.0 noch gültig ist, aktivieren Sie die Programmversion 9.0 mit dem Aktivierungscode von Version 8.0 (s. Abschnitt "Programm aktivieren" auf S. 23).
11. Starten Sie das Gerät neu, um die Installation abzuschließen.

ERSTE SCHRITTE

Dieser Abschnitt informiert darüber, wie Kaspersky Mobile Security 9.0 für den Einsatz vorbereitet wird (Programm aktivieren und Geheimcode festlegen), das Programm gestartet und das Gerät auf Viren untersucht wird.

IN DIESEM ABSCHNITT

Programm aktivieren 23

Geheimcode eingeben 27

Programm starten 28

Update der Programm-Datenbanken 28

Gerät auf Viren untersuchen 29

Programm-Info anzeigen 29

PROGRAMM AKTIVIEREN

Um mit Kaspersky Mobile Security 9.0 zu arbeiten, muss das Programm aktiviert werden. Bei der Programmaktivierung wird der Aktivierungscode eingegeben, der dann auf den Kaspersky-Lab-Servern geprüft und registriert wird. Anschließend lädt das Programm eine Schlüsseldatei herunter und installiert diese.

Ein Aktivierungscode kann folgendermaßen erworben werden:

- online (s. Abschnitt "Aktivierungscode online kaufen" auf S. 26). Dazu wird direkt aus Kaspersky Mobile Security 9.0 die Website http://www.kaspersky.com/gotopartnersite/def72/buy aufgerufen.
- auf der Webseite http://www.kaspersky.de/store
- im Fachhandel

Um Kaspersky Mobile Security auf einem Gerät zu aktivieren, ist eine Internetverbindung erforderlich.

Stellen Sie vor der Programmaktivierung sicher, dass Datum und Uhrzeit auf dem Smartphone korrekt eingestellt sind.

Das Programm kann auf folgende Weise aktiviert werden:

- **Testversion aktivieren**. Wählen Sie diese Aktivierungsmethode, wenn Sie das Programm zuerst testen und später eine kommerzielle Programmversion kaufen möchten. Bei der Aktivierung wird eine kostenlose Schlüsseldatei installiert. Die Gültigkeit der Testlizenz wird nach der Aktivierung auf dem Bildschirm angezeigt. Nach Ablauf der Testlizenz werden die Programmfunktionen eingeschränkt. Es stehen dann nur noch folgende Einstellungen zur Verfügung:
  - Programm aktivieren
  - Programmlizenzen verwalten
  - Hilfesystem für Kaspersky Mobile Security 9.0
  - Verschlüsselung deaktivieren
  - Privatsphäre deaktivieren

Es ist nicht möglich, eine weitere Testlizenz zu aktivieren.

- **Kommerzielle Version aktivieren**. Wählen Sie diese Variante, wenn Sie eine kommerzielle Programmversion erworben und einen Aktivierungscode erhalten haben. Nach Eingabe des Aktivierungscodes wird eine Schlüsseldatei empfangen und installiert. Nun können Sie das Programm im vollen Funktionsumfang nutzen. Die Gültigkeit der Lizenz wird auf dem Bildschirm angezeigt. Nach Ablauf der Gültigkeit wird die Programmfunktionalität eingeschränkt. Es wird keine Programmaktualisierung mehr ausgeführt.

IN DIESEM ABSCHNITT

Kommerzielle Version aktivieren....24

Testversion aktivieren....25

Aktivierungscode online kaufen....26

KOMMERZIELLE VERSION AKTIVIEREN

Gehen Sie folgendermaßen vor, um eine kommerzielle Programmversion mit einem Aktivierungscode zu aktivieren:

1. Öffnen Sie das Hauptmenü des Geräts.
2. Wählen Sie **Programme** → **Persönlich** → **KMS 9.0**.

   Der Installationsordner für das Programm kann je nach Modell des mobilen Geräts variieren.

3. Starten Sie das Programm. Gehen Sie dazu auf **Optionen** → **Öffnen**.

   Das Fenster **KMS 9.0** wird geöffnet.

4. Gehen Sie auf die Registerkarte **Erweitert** → **Lizenz** → **Code eingeben**.

   Das Aktivierungsfenster für Kaspersky Mobile Security 9.0 wird geöffnet.

5. Geben Sie den Code in die vier Felder ein. Der Aktivierungscode besteht aus Ziffern und lateinischen Buchstaben. Groß- und Kleinschreibung ist irrelevant. Gehen Sie nach der Eingabe des Aktivierungscodes auf **Optionen** → **Aktivieren** (s. Abb. unten).

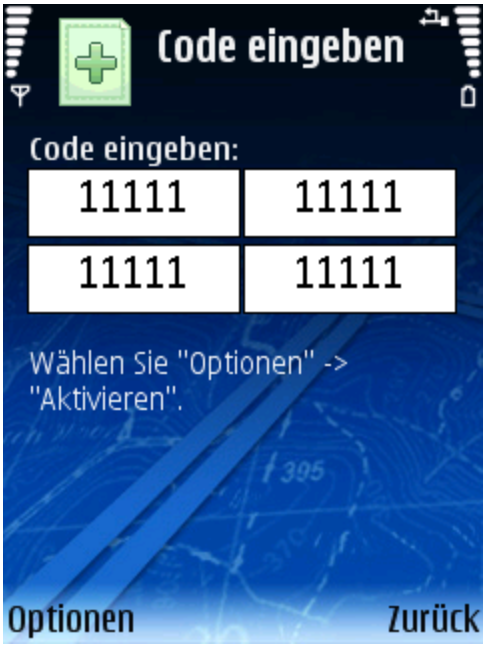


Abbildung 5. Kommerzielle Programmversion aktivieren

6. Bestätigen Sie die Internetverbindung mit **Ja**.

7. Wählen Sie einen Access Point für die Verbindung mit dem Aktivierungsserver von Kaspersky Lab.

   Das Programm sendet eine Anfrage an den Aktivierungsserver von Kaspersky Lab. Wenn der Aktivierungscode bestätigt wird, lädt das Programm eine Schlüsseldatei herunter und installiert sie.

   Wenn der von Ihnen eingegebene Aktivierungscode ungültig ist, erscheint eine entsprechende Meldung auf dem Bildschirm des mobilen Geräts. Prüfen Sie in diesem Fall, ob der Aktivierungscode richtig eingegeben wurde, und wenden Sie sich dann an die Firma, bei der Sie den Aktivierungscode für Kaspersky Mobile Security 9.0 gekauft haben.

   Wenn bei der Verbindung mit dem Server Fehler aufgetreten sind und der Download einer Schlüsseldatei fehlschlägt, wird die Aktivierung abgebrochen. In diesem Fall sollten die Einstellungen der Internetverbindung geprüft werden. Sollte es nicht gelingen, den Fehler zu beheben, wenden Sie sich an den technischen Support.

8. Gehen Sie zur Eingabe des Geheimcodes (s. Abschnitt "Geheimcode eingeben" auf S. 27).

TESTVERSION AKTIVIEREN

Gehen Sie folgendermaßen vor, um eine Testversion von Kaspersky Mobile Security 9.0 zu aktivieren:

1. Öffnen Sie das Hauptmenü des Geräts.

2. Wählen Sie **Programme** → **Persönlich** → **KMS 9.0**.

   Der Installationsordner für das Programm kann je nach Modell des mobilen Geräts variieren.

3. Starten Sie das Programm. Gehen Sie dazu auf **Optionen** → **Öffnen**.

   Das Fenster **KMS 9.0** wird geöffnet.

4. Gehen Sie auf die Registerkarte **Erweitert** → **Lizenz** → **Code eingeben**.

   Das Aktivierungsfenster für Kaspersky Mobile Security 9.0 wird geöffnet.

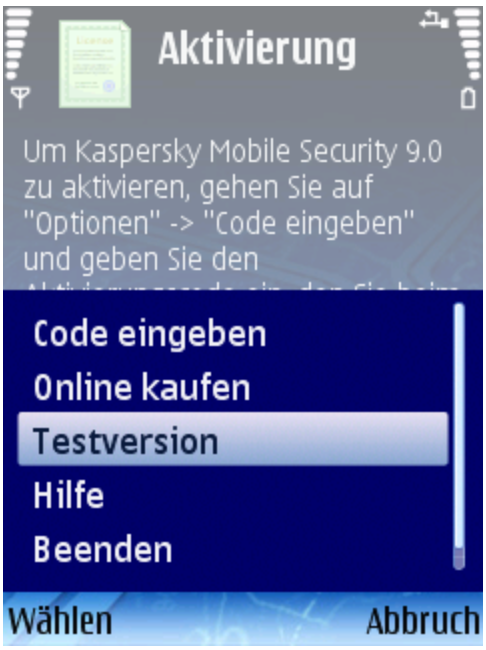


Abbildung 6. Testversion des Programms aktivieren

5. Bestätigen Sie die Internetverbindung mit **Ja**.

6. Wählen Sie einen Access Point für die Verbindung mit dem Server und klicken Sie dann auf **OK**.

   Das Programm sendet eine Anfrage an den Aktivierungsserver von Kaspersky Lab, lädt eine Schlüsseldatei herunter und installiert sie.

   Wenn bei der Verbindung mit dem Aktivierungsserver Fehler aufgetreten sind und keine Schlüsseldatei heruntergeladen wurde, wenden Sie sich an den technischen Support.

7. Gehen Sie zur Eingabe des Geheimcodes (s. Abschnitt "Geheimcode eingeben" auf S. 27).

AKTIVIERUNGSCODE ONLINE KAUFEN

Gehen Sie folgendermaßen vor, um im Online-Shop einen Aktivierungscode zu kaufen:

1. Öffnen Sie das Hauptmenü des Geräts.

2. Wählen Sie **Programme** → **Persönlich** → **KMS 9.0**.

   Der Installationsordner für das Programm kann je nach Modell des mobilen Geräts variieren.

3. Starten Sie das Programm. Gehen Sie dazu auf **Optionen** → **Beenden**.

   Das Fenster **KMS 9.0** wird geöffnet.

4. Gehen Sie auf **Optionen** → **Online kaufen**.

   Das Fenster **Online kaufen** wird geöffnet.

5. Klicken Sie auf **Öffnen** (s. Abb. unten).

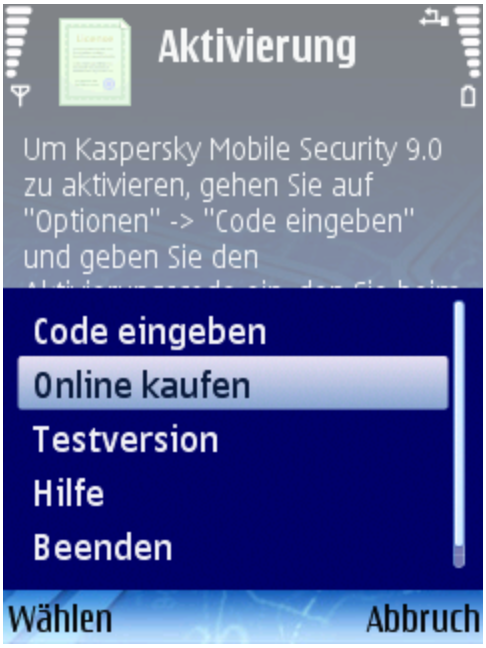


Abbildung 7. Aktivierungscode online kaufen

Die Webseite http://www.kaspersky.com/gotopartnersite/def72/buy wird geöffnet. Hier können Sie online ein Formular zum Kauf eines Aktivierungscodes ausfüllen.

6. Folgen Sie den einzelnen Schritten der Anweisung.

7. Nachdem Sie einen Aktivierungscode gekauft haben, gehen Sie zur Aktivierung einer kommerziellen Programmversion (s. Abschnitt "Kommerzielle Version aktivieren" auf S. 24).

GEHEIMCODE EINGEBEN

Nachdem das Programm aktiviert wurde, werden Sie aufgefordert, einen Geheimcode einzugeben. Der *Geheimcode* verhindert einen unautorisierten Zugriff auf die Programmeinstellungen. Der aktuelle Geheimcode kann später geändert werden.

Der Geheimcode wird in folgenden Fällen abgefragt:

- für den Zugriff auf das Programm
- für den Zugriff auf verschlüsselte Daten
- zur Aktivierung / Deaktivierung der Komponente *Privatsphäre*
- beim Senden eines Befehls mit Hilfe einer speziellen SMS-Nachricht für die Fernsteuerung folgender Funktionen: Blockieren, SMS-Clean, SIM-Watch, GPS-Find, Privatsphäre.
- bei der Deinstallation des Programms

Merken Sie sich den Geheimcode gut. Ohne Geheimcode können die Funktionen von Kaspersky Mobile Security nicht mehr ausgeführt werden, und es ist nicht mehr möglich, auf verschlüsselte Daten zuzugreifen und das Programm zu entfernen.

Ein Geheimcode sollte aus mindestens sieben Ziffern bestehen.

Gehen Sie folgendermaßen vor, um einen Geheimcode einzugeben:

1. Geben Sie im Feld **Neuen Code eingeben** die Ziffern ein, die Ihren Code bilden.
2. Wiederholen Sie die Eingabe im Feld **Code bestätigen**.

   Ein eingegebener Code wird automatisch auf seine Sicherheit geprüft.
3. Wenn die Prüfung ergibt, dass ein Code unsicher ist, erfolgt eine Warnung, und das Programm erfragt eine Bestätigung. Klicken Sie auf **Ja**, um den Code zu verwenden. Klicken Sie auf **Nein**, um einen neuen Code festzulegen.
4. Klicken Sie auf **OK**, um mit dem Programm zu arbeiten.

PROGRAMM STARTEN

Gehen Sie folgendermaßen vor, um Kaspersky Mobile Security 9.0 zu starten:

1. Öffnen Sie das Hauptmenü des Geräts.
2. Wählen Sie **Programme** → **Persönlich** → **KMS 9.0**.

   Der Installationsordner für das Programm kann je nach Modell des mobilen Geräts variieren.
3. Starten Sie das Programm. Gehen Sie dazu auf **Optionen** → **Öffnen**.

   Das Fenster **KMS 9.0** wird geöffnet.
4. Geben Sie den Geheimcode ein und klicken Sie auf **OK**.

Auf dem Bildschirm öffnet sich ein Fenster mit dem Schutzstatus von Kaspersky Mobile Security 9.0 (s. Abschnitt "Fenster für den Schutzstatus" auf S. 34). Klicken Sie auf **OK**, um zu den Optionen des Programms zu wechseln.

UPDATE DER PROGRAMM-DATENBANKEN

Bei der Suche nach Bedrohungen verwendet Kaspersky Mobile Security 9.0 die Programm-Datenbanken, die eine Beschreibung aller derzeit bekannten schädlichen Programme und entsprechende Desinfektionsmethoden sowie eine Beschreibung sonstiger unerwünschter Objekte enthalten. Die Datenbanken, die zum Lieferumfang von Kaspersky Mobile Security 9.0 gehören, können zum Zeitpunkt der Installation bereits veraltet sein.

Es wird empfohlen, die Datenbanken sofort nach der Programminstallation zu aktualisieren.

Um die Programm-Datenbanken zu aktualisieren, muss auf dem mobilen Gerät eine Internetverbindung eingerichtet sein.

Gehen Sie folgendermaßen vor, um das Update der Programm-Datenbanken manuell zu starten:

1. Wählen Sie auf der Registerkarte **Anti-Virus** den Punkt **Update**.

   Das Fenster **Update** wird geöffnet.
2. Gehen Sie auf **Update**.

Das Programm startet das Update der Datenbanken von einem Kaspersky-Lab-Server. Informationen über den Updatevorgang werden auf dem Bildschirm angezeigt.

GERÄT AUF VIREN UNTERSUCHEN

Es wird empfohlen, Ihr mobiles Gerät nach der Programminstallation vollständig auf schädliche Objekte zu untersuchen.

Die erste Untersuchung erfolgt mit von Kaspersky Lab vordefinierten Einstellungen.

Gehen Sie folgendermaßen vor, um eine vollständige Untersuchung des Geräts zu starten:

1. Wählen Sie auf der Registerkarte **Anti-Virus** den Punkt **Scan**.

   Das Fenster **Scan** wird geöffnet.

2. Wählen Sie **Alles scannen**.

PROGRAMM-INFO ANZEIGEN

Sie können allgemeine Informationen zum Programm, dessen Version und die Kopierberechtigungen anzeigen.

Um Informationen über das Programm anzuzeigen,

wählen Sie auf der Registerkarte **Erweitert** den Punkt **Programm-Infos**.

LIZENZVERWALTUNG

Im Zusammenhang mit der Lizenzierung von Kaspersky-Lab-Programmen sind folgende Begriffe wichtig:

- Lizenzvertrag
- Lizenz
- Schlüsseldatei

Diese drei Begriffe sind miteinander verbunden und bilden ein einheitliches Lizenzierungsschema.

Es folgt eine ausführliche Erklärung.

Dieser Abschnitt informiert außerdem darüber, wie Informationen zur Lizenz von Kaspersky Mobile Security 9.0 angezeigt werden können und wie die Nutzungsdauer der Lizenz verlängert wird.

IN DIESEM ABSCHNITT

Über den Lizenzvertrag 30

Über Lizenzen für Kaspersky Mobile Security 30

Über Schlüsseldateien für Kaspersky Mobile Security 30

Lizenz-Info anzeigen 31

Lizenz verlängern 32

ÜBER DEN LIZENZVERTRAG

Der *Lizenzvertrag* ist ein Vertrag zwischen einer natürlichen oder juristischen Person, die rechtmäßiger Besitzer eines Exemplars von Kaspersky Mobile Security ist, und der Kaspersky Lab ZAO. Der Lizenzvertrag gehört zum Lieferumfang jedes Kaspersky-Lab-Programms. Er legt die Rechte und Einschränkungen für die Nutzung von Kaspersky Mobile Security genau fest.

In Übereinstimmung mit dem Lizenzvertrag erhalten Sie durch den Erwerb und die Installation eines Kaspersky-Lab-Programms das unbefristete Besitzrecht an einer Kopie.

Kaspersky Lab bietet Ihnen folgende Zusatzleistungen an:

- Technischer Support
- Update der Datenbanken für Kaspersky Mobile Security
- Update der Programm-Module von Kaspersky Mobile Security

Um diese Leistungen zu nutzen, sind der Erwerb und die Aktivierung einer Lizenz erforderlich (s. Abschnitt "Über Lizenzen für Kaspersky Mobile Security" auf S. 30).

ÜBER LIZENZEN FÜR KASPERSKY MOBILE SECURITY

Die *Lizenz* verleiht das Recht zur Nutzung von Kaspersky Mobile Security und der zum Programm gehörenden Zusatzleistungen (s. Abschnitt "Über den Lizenzvertrag" auf S. 30), die von Kaspersky Lab und seinen Partnern angeboten werden.

Jede Lizenz wird durch die Gültigkeitsdauer und ihren Typ charakterisiert.

Die *Gültigkeitsdauer einer Lizenz* ist die Zeitspanne, für die Ihnen die Zusatzleistungen zur Verfügung stehen. Der Umfang der angebotenen Leistungen ist vom Lizenztyp abhängig.

Es sind folgende Lizenztypen vorgesehen:

Test – kostenlose Lizenz mit beschränkter Gültigkeitsdauer. Eine solche Lizenz dient zum Kennenlernen von Kaspersky Mobile Security. Sie wird zusammen mit einer Testversion des Programms geliefert und besitzt eine kurze Gültigkeitsdauer, während der Sie auf die Wissensdatenbank (http://support.kaspersky.de) und das Forum (http://forum.kaspersky.com/index.php?showforum=77) zugreifen können. Wenn Sie eine Testlizenz verwenden, können Sie den technischen Support nicht nutzen. Nach Ablauf der Gültigkeit stellt Kaspersky Mobile Security seine Funktion ein.

Kommerziell – gekaufte Lizenz, deren Gültigkeitsdauer i.d.R. ein Jahr beträgt. Eine Lizenz dieses Typs erhält der Benutzer beim Kauf des Programms. Nach Ablauf der Gültigkeit einer kommerziellen Lizenz stehen bestimmte Funktionen von Kaspersky Mobile Security nicht mehr zur Verfügung, und die Datenbanken werden nicht mehr aktualisiert. In diesem Fall ist für das Gerät kein umfassender Schutz mehr gewährleistet.

Um das Programm und die Zusatzleistungen zu verwenden, sind der Kauf und die Installation einer kommerziellen Lizenz erforderlich.

Eine Lizenz wird durch die Installation einer Schlüsseldatei aktiviert (s. Abschnitt "Über Schlüsseldateien für Kaspersky Mobile Security" auf S. 30).

ÜBER SCHLÜSSELDATEIEN FÜR KASPERSKY MOBILE SECURITY

Die *Schlüsseldatei* ist eine Datei, die Ihnen als persönlicher Schlüssel dient und für die Arbeit des Programms erforderlich ist. Die Schlüsseldatei realisiert auf technischem Weg die Aktivierung einer ihr entsprechenden Lizenz und damit Ihr Recht zur Nutzung des Programms und der Zusatzleistungen.

Eine Schlüsseldatei wird bei der Aktivierung durch einen Aktivierungscode automatisch erstellt.

Eine Schlüsseldatei enthält folgende Informationen:

- Gültigkeitsdauer der Lizenz
- Typ der Lizenz (Test, kommerziell)
- Lizenzbeschränkungen (z.B. auf welche Anzahl von Computern sich die Lizenz bezieht oder wie groß das Volumen des geschützten Mailverkehrs ist).
- Kontaktdaten des technischen Supports
- Gültigkeitsdauer der Schlüsseldatei

Die *Gültigkeitsdauer der Schlüsseldatei* gibt die "Haltbarkeitsdauer" an, die eine Schlüsseldatei bei ihrer Erstellung erhält. Das ist der Zeitraum, nach dessen Ablauf die Schlüsseldatei ungültig wird und die entsprechende Lizenz nicht mehr aktiviert werden kann.

Das folgende Beispiel erklärt das Verhältnis zwischen der Gültigkeitsdauer eines Schlüssels und der Gültigkeitsdauer einer Lizenz.

Beispiel:

Gültigkeitsdauer der Lizenz: 300 Tage

Erstellungsdatum der Schlüsseldatei: 01.09.2009

Gültigkeitsdauer der Schlüsseldatei: 300 Tage

Installationsdatum der Schlüsseldatei (Aktivierung der Lizenz): 10.09.09, d.h. 9 Tage nach dem Erstellungsdatum.

Ergebnis:

Resultierende Gültigkeitsdauer der Lizenz: 300 Tage minus 9 Tage = 291 Tage.

LIZENZ-INFO ANZEIGEN

Sie können folgende Informationen zur Lizenz erhalten: Schlüsseldatei, Typ, Anzahl der verbleibenden Tage und Gerätenummer.

Gehen Sie folgendermaßen vor, um Informationen zur Lizenz anzuzeigen:

1. Wählen Sie auf der Registerkarte **Erweitert** den Punkt **Lizenz**.

   Das Fenster **Lizenz** wird geöffnet.

2. Gehen Sie auf den Punkt **Lizenz-Info** (s. Abb. unten).

Abbildung 8. Lizenz-Info anzeigen

Das Fenster **Lizenz-Info** wird geöffnet.

LIZENZ VERLÄNGERN

Kaspersky Mobile Security 9.0 erlaubt es, die Programmlizenz zu erneuern.

Eine Lizenz kann auf folgende Weise verlängert werden:

- **Online** – Programm auf einer speziellen Website für ein Jahr aktivieren.
- **Mit Aktivierungscode** – Programm mit einem Aktivierungscode aktivieren. Einen Aktivierungscode können Sie auf der Seite http://www.kaspersky.de/store oder bei den Vertriebspartnern von Kaspersky Lab erwerben.

Um das Programm zu aktivieren, muss auf dem mobilen Gerät eine Internetverbindung eingerichtet sein.

IN DIESEM ABSCHNITT

Lizenz mit Aktivierungscode verlängern 32

Lizenz online verlängern 33

LIZENZ MIT AKTIVIERUNGSCODE VERLÄNGERN

Gehen Sie folgendermaßen vor, um die Lizenz mit einem Aktivierungscode zu verlängern:

1. Wählen Sie auf der Registerkarte **Erweitert** den Punkt **Lizenz**.

   Das Fenster **Lizenz** wird geöffnet.

2. Wählen Sie den Punkt **Code eingeben**.

Das Fenster **Code eingeben** wird geöffnet.

3. Geben Sie den Code in die entsprechenden vier Felder ein und gehen Sie dann auf **Optionen** → **Aktivieren** (s. Abb. unten).

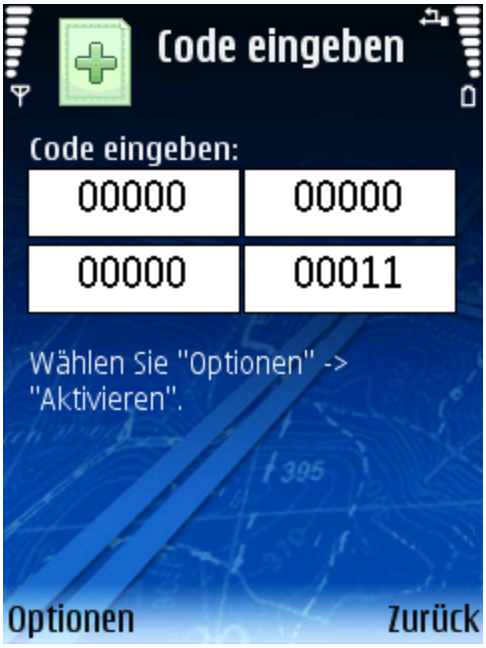


Abbildung 9. Lizenz mit Aktivierungscode verlängern

4. Wenn das Programm nach einem Access Point fragt, wählen sie aus der Liste den erforderlichen Verbindungstyp.

   Das Programm sendet eine Anfrage an den Aktivierungsserver von Kaspersky Lab, lädt automatisch eine Schlüsseldatei herunter und installiert sie. Wenn die Installation der Schlüsseldatei erfolgreich verläuft, werden auf dem Bildschim Informationen über die Lizenz angezeigt.

   Wenn der von Ihnen eingegebene Aktivierungscode ungültig ist, erscheint eine entsprechende Meldung auf dem Bildschim.

5. Klicken Sie zum Abschluss auf **OK**.

LIZENZ ONLINE VERLÄNGERN

Gehen Sie folgendermaßen vor, um eine Lizenz online zu verlängem:

1. Wählen Sie auf der Registerkarte **Erweitert** den Punkt **Lizenz**.

   Das Fenster **Lizenz** wird geöffnet.

2. Gehen Sie auf **Online verlängern** (s. Abb. unten).

Der Menüpunkt heißt **Online kaufen**, wenn die Lizenz abgelaufen ist.

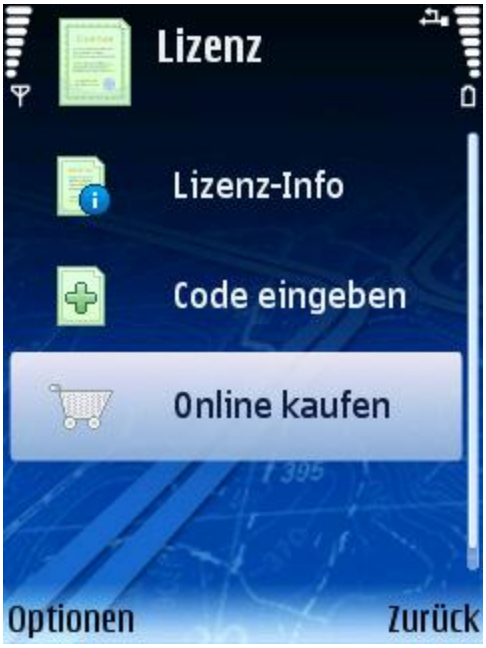


Abbildung 10. Lizenz online verlängern

Das Fenster **Online kaufen** wird geöffnet.

3. Klicken Sie auf **Öffnen**.

   Es wird eine Website geöffnet, auf der Sie ein Formular zur Lizenzverlängerung ausfüllen können.

   Wenn die Lizenz abgelaufen ist, öffnet sich die Webseite http://www.kaspersky.com/gotopartnersite/def72/buy, auf der Sie online einen Aktivierungscode kaufen können.

4. Folgen Sie den einzelnen Schritten der Anweisung.

5. Nachdem Sie einen Aktivierungscode gekauft haben, geben Sie den Aktivierungscode ein (s. Abschnitt "Lizenz mit Aktivierungscode verlängern" auf S. 32).

PROGRAMMOBERFLÄCHE

Die Benutzeroberfläche von Kaspersky Mobile Security 9.0 ist intuitiv verständlich und bequem zu handhaben. Dieser Abschnitt informiert über ihre wichtigsten Elemente.

SCHUTZSYMBOL

Das Schutzsymbol informiert über den Programmstatus. Das aktive (farbige) Symbol bedeutet, dass der Schutz aktiviert ist. Ist das Symbol inaktiv (grau), dann wurde der Schutz angehalten, und alle Schutzkomponenten sind deaktiviert.

In der Grundeinstellung wird das Schutzsymbol nicht auf dem Bildschirm des Geräts angezeigt. Sie können die Einstellungen für die Darstellung des Symbols ändern (s. Abschnitt "Schutzsymbol anzeigen" auf S. 108).

FENSTER FÜR DEN SCHUTZSTATUS

Der Status der wichtigsten Programmkomponenten wird im Fenster für den Schutzstatus angezeigt.

Es gibt drei Varianten für den Status. Jeder Status wird durch eine bestimmte Farbe signalisiert. Die Farben entsprechen den Signalen einer Ampel. Grün bedeutet, dass der Schutz Ihres Geräts dem erforderlichen Niveau entspricht. Gelb und Rot signalisieren, dass Sicherheitsrisiken vorliegen. Als Bedrohung gilt nicht nur der Fund schädlicher Programme, sondern auch die Verwendung veralteter Datenbanken, deaktivierte Schutzkomponenten, die Auswahl einer niedrigen Sicherheitsstufe u.a.

Das Fenster für den Schutzstatus ist sofort nach dem Programmstart verfügbar und bietet folgende Informationen:

- **Schutz** – Status des Echtzeitschutzes (s. Abschnitt "Schutz für das Dateisystem " auf S. 37).

  Grün bedeutet, dass der Schutz aktiviert ist und dem erforderlichen Niveau entspricht. Die Programm-Datenbanken sind aktuell.

  Gelb zeigt an, dass die Datenbanken seit mehreren Tagen nicht aktualisiert wurden.

  Rot signalisiert Probleme, die zu Datenverlust oder zur Infektion des Geräts führen können. Beispiel: Der Schutz ist deaktiviert. Möglicherweise wurde das Programm längere Zeit nicht aktualisiert.

- **Firewall** – Stufe für den Schutz des Geräts vor unerwünschter Netzwerkaktivität (s. Abschnitt "Filterung der Netzwerkaktivität. Firewall" auf S. 90).

  Das grüne Statussymbol bedeutet, dass die Komponente aktiviert ist. Es wurde eine Sicherheitsstufe für die Firewall ausgewählt.

  Rot zeigt an, dass die Netzwerkaktivität nicht gefiltert wird.

- **Diebstahlschutz** – Status des Schutzes bei Diebstahl oder Verlust des Geräts (s. Abschnitt "Datenschutz bei Verlust oder Diebstahl des Geräts" auf S. 72).

  Das grüne Statussymbol bedeutet, dass die Diebstahlschutz-Funktionen, die unter dem Status der Komponente angezeigt werden, aktiviert sind.

  Rot zeigt an, dass alle Funktionen des Diebstahlschutzes deaktiviert sind.

- **Privatsphäre** – Status des Schutzes für sensible Daten (s. Abschnitt "Private Daten verbergen" auf S. 82).

  Das grüne Statussymbol bedeutet, dass die Komponente aktiviert ist. Vertrauliche Daten werden verborgen.

  Gelb warnt davor, dass die Komponente deaktiviert ist. Persönliche Daten werden angezeigt und sind zur Anzeige verfügbar.

- **Lizenz** – Gültigkeitsdauer der Lizenz (s. Abschnitt "Lizenzverwaltung" auf S. 29).

  Das grüne Statussymbol bedeutet, dass die Lizenz noch mehr als 14 Tage gültig ist.

  Gelb warnt davor, dass die Lizenz weniger als 14 Tage gültig ist.

Rot signalisiert, dass die Gültigkeit der Lizenz abgelaufen ist.

Abbildung 11. Fenster für den Schutzstatus

Sie können auch in das Fenster für den Schutzstatus wechseln. Wählen Sie dazu **Optionen → Schutzstatus**.

In der Grundeinstellung wird das Fenster für den Schutzstatus sofort nach dem Programmstart angezeigt. Sie können die Darstellungseinstellungen ändern (s. Abschnitt "Statusfenster anzeigen" auf S. 107).

REGISTERKARTEN DES PROGRAMMS

Die Programmkomponenten sind logisch angeordnet und stehen auf den Registerkarten des Programms zur Verfügung. Jede Registerkarte bietet Zugriff auf die Einstellungen der gewählten Komponente oder auf die Schutzaufgaben.

Kaspersky Mobile Security 9.0 besitzt folgende Registerkarten:

- **Anti-Virus** – Schutz für das Dateisystem, Untersuchung und Update der Programm-Datenbanken
- **Privatsphäre** – vertrauliche Daten auf dem Gerät verbergen
- **Diebstahlschutz** – Bei Diebstahl oder Verlust das Gerät blockieren und Daten löschen
- **Verschlüsselung** – Datenverschlüsselung zum Schutz der Informationen auf dem Gerät
- **Anti-Spam** – Filterung von unerwünschten eingehenden Anrufen und SMS-Nachrichten
- **Kindersicherung** – Kontrolle über ausgehende Anrufe und SMS-Nachrichten
- **Firewall** – Netzwerkschutz für das Gerät
- **Erweitert** – allgemeine Programmeinstellungen, Informationen zum Programm, den verwendeten Datenbanken und der Lizenz

Die Registerkarten des Programms sind in der Grundeinstellung nach der Anzeige des Fensters mit dem Schutzstatus verfügbar (s. Abschnitt "Fenster für den Schutzstatus" auf S. 34).

Zur Navigation zwischen den Registerkarten bestehen folgende Möglichkeiten:

- mit dem Joystick oder den Navigationstasten des Geräts
- durch Auswahl von **Optionen** → **Registerkarte öffnen**

PROGRAMM-MENÜ

Das Programm-Menü bietet Zugriff auf die wichtigsten Aktionen. Das Menü enthält folgende Punkte (s. Abb. unten):

- **Auswählen** – Funktion, Befehl oder Parameter wählen
- **Registerkarte öffnen** – zur Auswahl einer Programmkomponente gehen
- **Schutzstatus** – Fenster für den Schutzstatus öffnen
- **Hilfe** – Kontexthilfe für Kaspersky Mobile Security 9.0 öffnen
- **Programm-Infos** – Fenster mit Informationen zum Programm anzeigen
- **Beenden** – Kaspersky Mobile Security 9.0 beenden

Abbildung 12. Programm-Menü

➧ *Um das Programm-Menü zu öffnen,*

gehen Sie auf **Optionen**.

Verwenden Sie zur Navigation innerhalb des Programm-Menüs den Joystick oder die Navigationstasten des Geräts.

SCHUTZ FÜR DAS DATEISYSTEM

Dieser Abschnitt informiert über den Schutz, der das Dateisystem Ihres Geräts vor Infektionen schützt. Außerdem wird beschrieben, wie der Schutz aktiviert / angehalten wird und wie die Schutzeinstellungen angepasst werden.

IN DIESEM ABSCHNITT

Schutz 38

Schutz aktivieren / deaktivieren 38

Schutzbereich anpassen 39

Aktion für gefundene Objekte wählen 40

Standardmäßige Schutzeinstellungen wiederherstellen 41

SCHUTZ

Der Schutz wird beim Hochfahren des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Geräts und untersucht alle Dateien, die geöffnet, gespeichert und gestartet werden. Der Untersuchungsvorgang für eine Datei wird nach folgendem Ablauf ausgeführt:

1. Die Komponente fängt den Zugriff des Benutzers oder eines Programms auf eine beliebige Datei ab.

2. Eine Datei wird auf schädliche Objekte analysiert. Schädliche Objekte werden auf Basis der Programm-Datenbanken erkannt. Die Datenbanken enthalten eine Beschreibung aller momentan bekannten schädlichen Objekte und entsprechende Desinfektionsmethoden.

3. Aufgrund der Analyseergebnisse bestehen folgende Varianten für das Verhalten von Kaspersky Mobile Security 9.0:

   - Wenn in einer Datei Schadcode gefunden wird, sperrt das Programm die Datei und führt die festgelegte Aktion aus.

   - Wenn in einer Datei kein schädlicher Code gefunden wird, erhält der Benutzer sofort Zugriff auf die Datei.

Informationen über die Untersuchungsergebnisse werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. 103).

SCHUTZ AKTIVIEREN / DEAKTIVIEREN

Wenn der Schutz aktiviert ist, werden alle Aktionen in Ihrem System permanent kontrolliert. Der Virenschutz beansprucht die Ressourcen des Geräts. Wenn mehrere Aufgaben ausgeführt werden, kann der Schutz vorübergehend angehalten werden, um die Auslastung des Geräts zu senken.

Die Kaspersky-Lab-Spezialisten warnen ausdrücklich davor, den Schutz zu deaktivieren, weil dies zur Infektion Ihres Geräts und zu Datenverlust führen kann.

Der aktuelle Status des Schutzes wird auf der Registerkarte **Anti-Virus** neben dem Menüpunkt **Schutz** angezeigt.

Um die Parameterwerte zu ändern, verwenden Sie den Joystick oder die Navigationstasten des Geräts oder gehen Sie auf **Optionen** → **Ändern**.

➧ *Gehen Sie folgendermaßen vor, um den Schutz zu aktivieren:*

1. Wählen Sie auf der Registerkarte **Anti-Virus** den Punkt **Schutz**.

   Das Fenster **Schutz** wird geöffnet.

2. Wählen Sie für **Schutzmodus** den Wert **An** (s. Abb. unten).

Abbildung 13. Schutz aktivieren

3. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

Gehen Sie folgendermaßen vor, um den Schutz zu deaktivieren:

1. Wählen Sie auf der Registerkarte **Anti-Virus** den Punkt **Schutz**.

   Das Fenster **Schutz** wird geöffnet.

2. Wählen Sie für **Schutzmodus** den Wert **Aus**.

3. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

SCHUTZBEREICH ANPASSEN

In der Grundeinstellung untersucht Kaspersky Mobile Security 9.0 alle Dateitypen. Um die Untersuchungsdauer zu verkürzen, können Sie einen Typ für die Untersuchungsobjekte festlegen.

Um die Parameterwerte zu ändern, verwenden Sie den Joystick oder die Navigationstasten des Geräts oder gehen Sie auf **Optionen → Ändern**.

Gehen Sie folgendermaßen vor, um einen Typ für die Untersuchungsobjekte zu wählen:

1. Wählen Sie auf der Registerkarte **Anti-Virus** den Punkt **Schutz**.

   Das Fenster **Schutz** wird geöffnet.

2. Wählen Sie einen Wert für **Scan-Objekte** (s. Abb. unten):

   - **Alle Dateien** – alle Dateitypen untersuchen.

- **Ausführbare** – nur ausführbare Programmdateien untersuchen (z.B. die Dateiformate *.exe, *.sis, *.mdl, *.app).

Abbildung 14. Schutzobjekte wählen

3. Klicken Sie auf **OK**, um die Änderungen zu speichern.

AKTION FÜR GEFUNDENE OBJEKTE WÄHLEN

In der Grundeinstellung werden gefundene schädliche Objekte von Kaspersky Mobile Security 9.0 in die Quarantäne verschoben. Die Aktion, die das Programm beim Fund eines schädlichen Objekts ausführen soll, kann geändert werden.

Um die Parameterwerte zu ändern, verwenden Sie den Joystick oder die Navigationstasten des Geräts oder gehen Sie auf **Optionen → Ändern**.

Gehen Sie folgendermaßen vor, um die Reaktion des Programms auf ein schädliches Objekt einzustellen.

1. Wählen Sie auf der Registerkarte **Anti-Virus** den Punkt **Schutz**.

   Das Fenster **Schutz** wird geöffnet.

2. Legen Sie fest, welche Aktion das Programm beim Fund eines schädlichen Objekts ausführen soll. Wählen Sie dazu einen Wert für **Bei Virenfund** (s. Abb. unten):

   - **Löschen** – schädliche Objekte löschen, ohne den Benutzer zu benachrichtigen.
   - **Nach Quarantäne** – Objekte in die Quarantäne verschieben.

- **Protokollieren** – schädliche Objekte überspringen und Fund in den Programmbericht eintragen. Versuche zum Zugriff auf ein Objekt (z.B. Kopieren oder Öffnen) werden blockiert.

Abbildung 15. Reaktion des Programms auf den Fund eines schädlichen Objekts

3. Klicken Sie auf **OK**, um die Änderungen zu speichern.

STANDARDMÄSSIGE SCHUTZEINSTELLUNGEN WIEDERHERSTELLEN

Der Schutz arbeitet standardmäßig mit den von Kaspersky Lab empfohlenen Einstellungen. Sie können jederzeit zu den empfohlenen Einstellungen für den Schutz zurückkehren.

➧ *Gehen Sie folgendermaßen vor, um die standardmäßigen Schutzeinstellungen wiederherzustellen,*

1. Wählen Sie auf der Registerkarte **Anti-Virus** den Punkt **Schutz**.

   Das Fenster **Schutz** wird geöffnet.

2. Gehen Sie auf **Optionen** → **Wiederherstellen**.

UNTERSUCHUNG DES GERÄTS

Dieser Abschnitt informiert über die Virenuntersuchung. Sie erlaubt es, auf Ihrem Gerät Bedrohungen zu finden und zu neutralisieren. Außerdem werden hier folgende Vorgänge beschrieben: Untersuchungsaufgabe starten, Zeitplan für den Aufgabenstart erstellen, Untersuchungsobjekte wählen, Aktion des Programms für den Fund einer Bedrohung festlegen.

IN DIESEM ABSCHNITT

Über die Untersuchung des Geräts 42

Untersuchung manuell starten 42

Untersuchung nach Zeitplan starten 44

Typ der Untersuchungsobjekte wählen 45

Aktion für gefundene Objekte wählen 46

Archiv-Untersuchung anpassen 48

Standardmäßige Einstellungen für die Untersuchung des Geräts wiederherstellen 49

ÜBER DIE UNTERSUCHUNG DES GERÄTS

Mit der Untersuchung des Geräts lassen sich schädliche Objekte auf Ihrem Gerät erkennen und neutralisieren. Mit Kaspersky Mobile Security 9.0 kann das Dateisystem des Geräts vollständig oder teilweise untersucht werden, d.h. die Untersuchung lässt sich auf den Inhalt des Gerätespeichers, der Nachrichten oder eines bestimmten Ordners (auch eines Ordners auf einer Speicherkarte) beschränken.

Die Untersuchung des Geräts wird nach folgendem Ablauf ausgeführt:

1. Kaspersky Mobile Security 9.0 untersucht die Dateien der festgelegten Typen (s. Abschnitt "Typ der Untersuchungsobjekte wählen" auf S. 45).

2. Eine Datei wird auf schädliche Objekte analysiert. Kaspersky Mobile Security 9.0 erkennt schädliche Objekte auf Basis der Programm-Datenbanken. Die Datenbanken enthalten eine Beschreibung aller momentan bekannten schädlichen Objekte und entsprechende Desinfektionsmethoden.

   Aufgrund der Analyseergebnisse bestehen folgende Varianten für das Vorgehen von Kaspersky Mobile Security 9.0:

   - Wenn in einer Datei ein schädliches Objekt gefunden wird, führt Kaspersky Mobile Security 9.0 die festgelegte Aktion aus (s. Abschnitt "Aktion für gefundene Objekte wählen" auf S. 46).

   - Wenn kein schädlicher Code gefunden wird, wird die Datei sofort zum Zugriff freigegeben.

Eine Untersuchungsaufgabe kann manuell oder automatisch nach einem zuvor erstellten Zeitplan (s. Abschnitt "Untersuchung nach Zeitplan starten" auf S. 44) gestartet werden.

Informationen über die Ergebnisse des Scans auf Befehl werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. 103).

UNTERSUCHUNG MANUELL STARTEN

Sie können die Untersuchung manuell starten, wenn das Gerät gerade nicht mit anderen Aufgaben beschäftigt ist.

➧ *Gehen Sie folgendermaßen vor, um die Virenuntersuchung manuell zu starten:*

1. Wählen Sie auf der Registerkarte **Anti-Virus** den Punkt **Scan**.

   Das Fenster **Scan** wird geöffnet.

2. Wählen Sie einen Untersuchungsbereich für das Gerät (s. Abb. unten):

- **Alles scannen** – gesamtes Dateisystem des Geräts untersuchen. Standardmäßig werden folgende Objekte untersucht: Gerätespeicher und Speicherkarten.

- **Ordner scannen** – einzelnes Objekt im Dateisystem des Geräts oder auf einer Speicherkarte untersuchen. Durch Klick auf **Ordner scannen** öffnet sich ein Fenster, in dem das Dateisystem des Geräts dargestellt ist. Verwenden Sie zur Navigation im Dateisystem den Joystick oder die Navigationstasten. Markieren Sie den gewünschten Ordner und gehen Sie auf **Optionen → Scannen**, um die Untersuchung eines Ordners zu starten.

- **Speicher scannen** – im Systemspeicher laufende Prozesse und die dazu gehörenden Dateien untersuchen.

- **Nachr. scannen** – per SMS, MMS und Bluetooth empfangene Nachrichten untersuchen.

Abbildung 16. Untersuchungsbereich wählen

Nach dem Start der Untersuchung öffnet sich ein Untersuchungsfenster, das folgende Angaben zum aktuellen Status enthält: Anzahl der untersuchten Objekte, Pfad des momentan untersuchten Objekts und Fortschrittsanzeige mit Prozentangabe (s. Abb. unten).

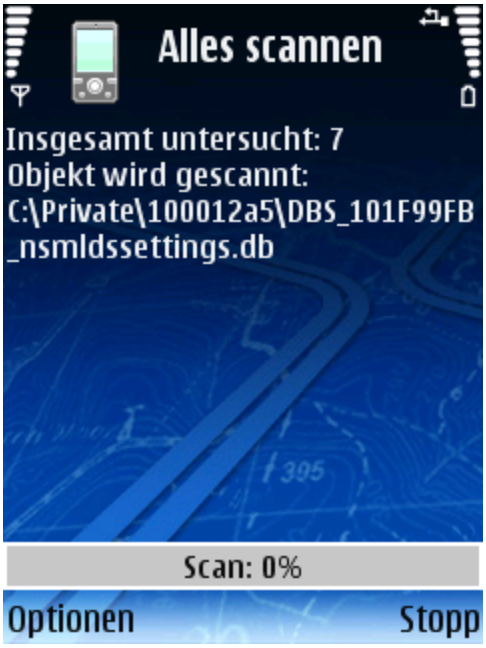


Abbildung 17. Status der Untersuchung des Geräts

Beim Fund eines schädlichen Objekts führt Kaspersky Mobile Security 9.0 die in den Untersuchungseinstellungen festgelegte Aktion aus (s. Abschnitt "Aktion für gefundene Objekte wählen" auf S. 46).

Wenn Kaspersky Mobile Security 9.0 eine Bedrohung findet, versucht er diese standardmäßig zu desinfizieren. Wenn eine Desinfektion nicht möglich ist, wird das gefundene Objekt in die Quarantäne verschoben.

Nach Abschluss der Untersuchung erscheint auf dem Bildschirm eine Statistik mit folgendem Inhalt:

- Anzahl der untersuchten Objekte
- Anzahl der gefundenen, unter Quarantäne gestellten und gelöschten Viren
- Anzahl der übersprungenen Objekte (Beispiele: *Datei wird vom Betriebssystem verwendet* oder *Keine ausführbare Datei*, wenn nur ausführbare Dateien untersucht werden).
- Zeitpunkt der Untersuchung

In der Grundeinstellung wird während einer Untersuchung die Hintergrundbeleuchtung automatisch ausgeschaltet, um den Akku zu schonen. Die Einstellungen der Hintergrundbeleuchtung können angepasst werden (s. Abschnitt "Hintergrundbeleuchtung verwalten" auf S. 106).

UNTERSUCHUNG NACH ZEITPLAN STARTEN

Mit Kaspersky Mobile Security 9.0 kann ein Zeitplan eingerichtet werden, nach dem die Untersuchung automatisch zur angegebenen Zeit startet. Die Untersuchung erfolgt im Hintergrund. Wenn ein infiziertes Objekt gefunden wird, führt das Programm die Aktion aus, die in den Untersuchungsparametern festgelegt wurde.

Der Start einer geplanten Untersuchung ist in der Grundeinstellung deaktiviert.

➧ *Gehen Sie folgendermaßen vor, um einen Untersuchungszeitplan anzupassen:*

1. Wählen Sie auf der Registerkarte **Anti-Virus** den Punkt **Scan**.

Das Fenster **Scan** wird geöffnet.

2. Gehen Sie auf **Zeitplan**.

   Das Fenster **Zeitplan** wird geöffnet.

3. Legen Sie einen Wert für **Auto-Scan** fest (s. Abb. unten):

   - **Aus** – Start der Untersuchung nach Zeitplan ausschalten.
   - **Wöchentlich** - Die Untersuchung erfolgt einmal pro Woche. Geben Sie **Scan-Tag** und **Scan-Zeit** an.
   - **Täglich** - Die Untersuchung erfolgt jeden Tag. Geben Sie im Eingabefeld die **Scan-Zeit** an.

Abbildung 18. Untersuchung nach Zeitplan anpassen

4. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

TYP DER UNTERSUCHUNGSOBJEKTE WÄHLEN

In der Grundeinstellung untersucht Kaspersky Mobile Security 9.0 alle Dateien, die sich auf dem Gerät und auf der Speicherkarte befinden. Um die Untersuchungsdauer zu verkürzen, können Sie einen Typ für die Untersuchungsobjekte wählen, d.h. das Format der Dateien festlegen, die auf Schadcode gescannt werden sollen.

Um die Parameterwerte zu ändern, verwenden Sie den Joystick oder die Navigationstasten des Geräts oder gehen Sie auf **Optionen → Ändern**.

Gehen Sie folgendermaßen vor, um Untersuchungsobjekte zu wählen:

1. Wählen Sie auf der Registerkarte **Anti-Virus** den Punkt **Scan**.

   Das Fenster **Scan** wird geöffnet.

2. Gehen Sie auf **Objekte / Aktionen**.

   Das Fenster **Objekte / Aktionen** wird geöffnet.

3. Wählen Sie einen Wert für den Parameter **Scan-Objekte** (s. Abb. unten):

   - **Alle Dateien** – alle Dateitypen untersuchen, Archive entpacken und deren Inhalt untersuchen. Es werden Archive der folgenden Formaten gescannt: *.zip, *.sis, *.cab und *.sisx.

   - **Ausführbare** – nur ausführbare Programmdateien folgender Formate untersuchen: *.exe, *.dll, *.sis, *.mdl, *.app, * .rdl, *.prt, *.pxt, *.ldd, *.pdd, *.class. Dabei werden Archive nicht entpackt und nicht untersucht.

Abbildung 19. Typ der Untersuchungsobjekte wählen

4. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

AKTION FÜR GEFUNDENE OBJEKTE WÄHLEN

In der Grundeinstellung werden gefundene infizierte Objekte von Kaspersky Mobile Security 9.0 in die Quarantäne verschoben. Sie können festlegen, wie das Programm beim Fund eines schädlichen Objekts reagieren soll.

Um die Parameterwerte zu ändern, verwenden Sie den Joystick oder die Navigationstasten des Geräts oder gehen Sie auf **Optionen → Ändern**.

Um die Reaktion des Programms anzupassen, gehen Sie folgendermaßen vor:

1. Wählen Sie auf der Registerkarte **Anti-Virus** den Punkt **Scan**.

   Das Fenster **Scan** wird geöffnet.

2. Gehen Sie auf **Objekte / Aktionen**.

   Das Fenster **Objekte/Aktionen** wird geöffnet.

3. Legen Sie eine Aktion für schädliche Objekte fest. Wählen Sie dazu einen Wert für **Bei Virenfund** (s. Abb. unten):

   - **Löschen** – gefundene schädliche Objekte löschen, ohne den Benutzer zu benachrichtigen.

   - **Nach Quarantäne** – gefundene schädliche Objekte in die Quarantäne verschieben.

- **Aktion erfragen** – Benutzer nach einer Aktion fragen. Beim Fund einer Bedrohung erfolgt eine Aktionsabfrage.

- **Protokollieren** – schädliche Objekte überspringen und Fund in den Programmbericht eintragen. Versuche zum Zugriff auf ein Objekt (z.B. Kopieren oder Öffnen) werden blockiert.

- **Desinfektionsversuch** – schädliche Objekte desinfizieren. Wenn die Desinfektion fehlschlägt, wird die Aktion ausgeführt, die für **Wenn irreparabel** gewählt wurde.

Abbildung 20. Aktion für schädliches Objekt wählen

4. Wenn Sie den Wert **Desinfektionsversuch** gewählt haben, legen Sie eine zweite Aktion des Programms fest, die ausgeführt werden soll, falls ein gefundenes Objekt nicht desinfiziert werden kann. Wählen Sie dazu einen Wert für **Wenn irreparabel** (s. Abb. unten):

    - **Löschen** – schädliche Objekte löschen, ohne den Benutzer zu benachrichtigen.

    - **Nach Quarantäne** – Objekte in die Quarantäne verschieben.

    - **Aktion erfragen** – beim Fund von schädlichen Objekten den Benutzer nach einer Aktion fragen.

- **Protokollieren** – schädliche Objekte überspringen und Fund in den Programmbericht eintragen. Versuche zum Zugriff auf ein Objekt (z.B. Kopieren oder Öffnen) werden blockiert.

Abbildung 21. Aktion für irreparable Schadobjekte wählen

5. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

ARCHIV-UNTERSUCHUNG ANPASSEN

Viren werden häufig in Archiven versteckt. Um den Inhalt von Archiven zu untersuchen, müssen diese entpackt werden. Das kann sich negativ auf die Leistungsfähigkeit des Geräts auswirken.

In der Grundeinstellung ist das Entpacken von Archiven aktiviert. Das Programm scannt Archive der folgenden Formate: *.zip, *.sis, *.sisx, *.cab. Um die Untersuchung zu beschleunigen, können Sie das Entpacken von Archiven ausschalten.

Um die Parameterwerte zu ändern, verwenden Sie den Joystick oder die Navigationstasten des Geräts oder gehen Sie auf **Optionen → Ändern**.

➧ *Gehen Sie folgendermaßen vor, um das Entpacken von Archiven zu deaktivieren:*

1. Wählen Sie auf der Registerkarte **Anti-Virus** den Punkt **Scan**.

   Das Fenster **Scan** wird geöffnet.

2. Gehen Sie auf **Objekte / Aktionen**.

   Das Fenster **Objekte / Aktionen** wird geöffnet.

3. Wählen Sie für **Archive entpacken** den Wert **Nein** (s. Abb. unten).

Abbildung 22. Archiv-Untersuchung anpassen

4. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

STANDARDMÄSSIGE EINSTELLUNGEN FÜR DIE UNTERSUCHUNG DES GERÄTS WIEDERHERSTELLEN

Die Untersuchung des Geräts erfolgt standardmäßig mit den von Kaspersky Lab empfohlenen Einstellungen. Sie können jederzeit zu den empfohlenen Einstellungen für die Untersuchung des Geräts zurückkehren.

Gehen Sie folgendermaßen vor, um die standardmäßigen Einstellungen für die Untersuchung des Geräts wiederherzustellen:

1. Wählen Sie auf der Registerkarte **Anti-Virus** den Punkt **Scan**.

   Das Fenster **Scan** wird geöffnet.

2. Gehen Sie auf **Objekte / Aktionen**.

   Das Fenster **Objekte / Aktionen** wird geöffnet.

3. Gehen Sie auf **Optionen** → **Wiederherstellen**.

QUARANTÄNE FÜR MÖGLICHERWEISE INFIZIERTE OBJEKTE

Dieser Abschnitt informiert über den speziellen Speicher *Quarantäne*, in den potentiell gefährliche Objekte verschoben werden. Außerdem wird hier die Arbeit mit Quarantäneobjekten beschrieben: Quarantäneobjekte anzeigen, wiederherstellen oder löschen.

IN DIESEM ABSCHNITT

Quarantäne 50

Quarantäneobjekte anzeigen 50

Quarantäneobjekte wiederherstellen 51

Quarantäneobjekte löschen 51

QUARANTÄNE

Die Quarantäne ist ein spezieller Ordner, in den Kaspersky Mobile Security 9.0 potentiell gefährliche Objekte verschiebt.

Schädliche Objekte können bei einer Untersuchung des Geräts oder im Rahmen des Schutzes erkannt und unter Quarantäne gestellt werden.

Die in die Quarantäne verschobenen Objekte werden in gepackter Form gespeichert, so dass deren Aktivierung ausgeschlossen ist und von ihnen keine Gefahr mehr für das Gerät ausgeht. Die Objekte können später gelöscht oder wiederhergestellt werden.

QUARANTÄNEOBJEKTE ANZEIGEN

Sie können die Objekte, die in die Quarantäne verschoben wurden, anzeigen. Für jedes Objekt werden der vollständige Name und das Funddatum angezeigt.

- *Um eine Liste der Quarantäneobjekte anzuzeigen:*

  Wählen Sie auf der Registerkarte **Anti-Virus** den Punkt **Quarantäne**.

Das Fenster **Quarantäne** wird geöffnet. Es enthält eine Liste der Quarantäneobjekte (s. Abb. unten):

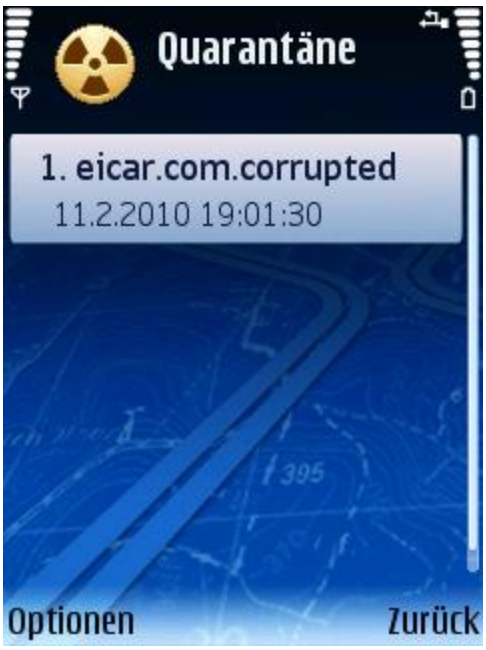


Abbildung 23. Liste der Quarantäneobjekte

QUARANTÄNEOBJEKTE WIEDERHERSTELLEN

Wenn Sie sicher sind, dass ein Objekt, das in die Quarantäne verschoben wurde, keine Gefahr für das Gerät darstellt, können Sie es aus der Quarantäne wiederherstellen. Ein wiederhergestelltes Objekt wird in den ursprünglichen Ordner verschoben.

- *Gehen Sie folgendermaßen vor, um ein Objekt aus der Quarantäne wiederherzustellen:*

1. Wählen Sie auf der Registerkarte **Anti-Virus** den Punkt **Quarantäne**.

   Das Fenster **Quarantäne** wird geöffnet.

2. Wählen Sie ein Objekt, das wiederhergestellt werden soll, und gehen Sie dann auf **Optionen** → **Wiederherstellen**.

QUARANTÄNEOBJEKTE LÖSCHEN

Es können ein oder alle Objekte, die in der Quarantäne gespeichert sind, gelöscht werden.

- *Gehen Sie folgendermaßen vor, um ein Objekt aus der Quarantäne zu löschen:*

1. Wählen Sie auf der Registerkarte **Anti-Virus** den Punkt **Quarantäne**.

   Das Fenster **Quarantäne** wird geöffnet.

2. Wählen Sie ein Objekt, das gelöscht werden soll, und gehen Sie dann auf **Optionen** → **Löschen**.

Das markierte Objekt wird gelöscht.

- *Gehen Sie folgendermaßen vor, um alle Quarantäneobjekte zu löschen:*

1. Wählen Sie auf der Registerkarte **Anti-Virus** den Punkt **Quarantäne**.

   Das Fenster **Quarantäne** wird geöffnet.

2. Gehen Sie auf **Optionen** → **Alle löschen**.

Alle Quarantäneobjekte werden gelöscht.

EINGEHENDE ANRUFE UND SMS-NACHRICHTEN FILTERN

Dieser Abschnitt informiert über die Komponente Anti-Spam, die eingehende Nachrichten und Anrufe aufgrund einer Schwarzen und Weißen Liste filtert. Außerdem werden hier folgende Vorgänge beschrieben: Schwarze und Weiße Liste anlegen, in Anti-Spam eine Aktion für eingehende Nachrichten und Anrufe festlegen, Komponente anpassen.

IN DIESEM ABSCHNITT

Anti-Spam 52

Über die Modi für Anti-Spam 53

Anti-Spam-Modus ändern 53

Schwarze Liste anlegen 54

Weiße Liste anlegen 57

Reaktion auf SMS-Nachrichten und Anrufe von Kontakten, die nicht im Telefonbuch stehen 60

Reaktion auf SMS-Nachrichten von Nicht-Ziffern-Nummern 61

Aktion für eingehende SMS-Nachrichten wählen 62

Aktion für eingehende Anrufe wählen 63

ANTI-SPAM

Anti-Spam schützt das Gerät vor unerwünschten Nachrichten und Anrufen. Anti-Spam filtert eingehende SMS-Nachrichten und Anrufe unter Verwendung einer schwarzen und weißen Liste.

Die Listen bestehen aus Einträgen. Jeder Eintrag kann folgende Parameter enthalten:

- Datentyp (SMS-Nachricht, Anruf, SMS-Nachricht und Anruf), auf den die Filterung angewendet wird (obligatorischer Parameter)
- Telefonnummer, von der die Daten stammen
- Text, den eine SMS-Nachricht enthalten kann

Anti-Spam filtert Nachrichten und Anrufe gemäß den festgelegten Einstellungen (s. Abschnitt "Über die Modi für Anti-Spam" auf S. 53). Nach diesen Einstellungen untersucht Anti-Spam alle eingehenden Anrufe und SMS-Nachrichten und stuft sie als erwünscht oder unerwünscht (Spam) ein. Sobald Anti-Spam einen Anruf oder eine SMS als erwünscht oder unerwünscht einstuft, wird die Untersuchung abgeschlossen.

Der Algorithmus für Anti-Spam umfasst standardmäßig folgende Schritte:

1. Untersuchung einer eingehenden SMS-Nachricht auf Übereinstimmung mit Telefonnummer und Text:
   a. Nach der Schwarzen Liste. Wenn die Liste einen Eintrag enthält, dessen Nummer und Text mit den Daten aus der eingehenden SMS-Nachricht übereinstimmen, wird die SMS-Nachricht als unerwünscht eingestuft und blockiert. Das Programm löscht die blockierte SMS-Nachricht.
   b. Nach der Weißen Liste. Wenn die Liste einen Eintrag enthält, dessen Nummer und Text mit den Daten aus der eingehenden SMS-Nachricht übereinstimmen, wird die SMS-Nachricht als erwünscht eingestuft und erlaubt.
2. Ein Anruf oder eine SMS-Nachricht wird nur auf Übereinstimmung mit einer Nummer untersucht:
   a. Nach der Schwarzen Liste. Wenn die Liste einen Eintrag enthält, dessen Nummer mit der Nummer des Absenders/Anrufers übereinstimmt, wird der Anruf oder die SMS als Spam eingestuft und blockiert. Das Programm löscht die blockierte SMS-Nachricht.

b. Nach der Weißen Liste. Wenn die Liste einen Eintrag enthält, dessen Nummer mit der Nummer des Absenders/Anrufers übereinstimmt (wobei im Eintrag kein Text angegeben ist), wird der Anruf oder die SMS als erwünscht eingestuft und erlaubt.

3. Eine Nachricht wird nur auf Übereinstimmung mit einem Text untersucht:

   a. Nach der Schwarzen Liste. Wenn die Liste einen Eintrag enthält, dessen Text mit den Daten aus der eingehenden SMS-Nachricht übereinstimmt (wobei im Eintrag keine Nummer angegeben ist), wird die SMS-Nachricht als Spam eingestuft und blockiert. Das Programm löscht die blockierte SMS-Nachricht.

   b. Nach der Weißen Liste. Wenn die Liste einen Eintrag enthält, dessen Text mit den Daten aus der eingehenden SMS-Nachricht übereinstimmt (wobei im Eintrag keine Nummer angegeben ist), wird die SMS-Nachricht als erwünscht eingestuft und erlaubt.

4. Aktion wählen. Wenn keine Übereinstimmung mit der Schwarzen oder Weißen Liste besteht, werden Anrufe und SMS-Nachrichten in der Grundeinstellung von Anti-Spam erlaubt, und im Meldungsfenster erfolgt eine Aktionsabfrage für Anrufe / Nachrichten. Außerdem enthält die Meldung folgende Zusatzinformationen: Für einen angenommenen Anruf wird die Nummer des Anrufers genannt. Für SMS-Nachrichten werden Telefonnummer und Nachrichteninhalt angegeben.

Informationen über blockierte SMS-Nachrichten und Anrufe werden in einem Bericht erfasst (s. Abschnitt "Programmberichte" auf S. 103).

ÜBER DIE MODI FÜR ANTI-SPAM

Ein Modus von Anti-Spam basiert auf einer Auswahl von Parametern, nach denen Ihr Gerät vor unerwünschten Meldungen und Anrufen geschützt wird.

Es sind folgende Modi für Anti-Spam vorgesehen:

- **Beide Listen** – Zur Filterung eingehender SMS-Nachrichten und Anrufe werden die Schwarze und die Weiße Liste verwendet. Wenn eine eingehende SMS oder ein Anruf von einer Nummer stammt, die auf keiner der beiden Listen steht, werden Sie darüber informiert. Sie können dann darüber entscheiden, ob eine SMS / ein Anruf erlaubt wird, ohne die Telefonnummer zu einer Liste hinzuzufügen, oder ob die Nummer in die Schwarze oder die Weiße Liste aufgenommen werden soll.

  Dieser Modus ist standardmäßig aktiviert.

- **Schwarze Liste** – SMS-Nachrichten und Anrufe von Nummern, die auf der Schwarzen Liste stehen, werden blockiert. Blockierte SMS-Nachrichten werden gelöscht. Alle übrigen SMS-Nachrichten und Anrufe werden erlaubt.

- **Weiße Liste** – SMS-Nachrichten und Anrufe von Nummern, die auf der Weißen Liste stehen, werden erlaubt. Alle übrigen SMS-Nachrichten und Anrufe werden blockiert. Blockierte SMS-Nachrichten werden gelöscht.

- **Aus** – SMS-Nachrichten und Anrufe nicht filtern.

Sie können den Modus für Anti-Spam ändern (s. Abschnitt "Anti-Spam-Modus ändern" auf S. 53). Der aktuelle Modus von Anti-Spam wird auf der Registerkarte **Anti-Spam** neben dem Menüpunkt **Modus** angezeigt.

ANTI-SPAM-MODUS ÄNDERN

Um die Parameterwerte zu ändern, verwenden Sie den Joystick oder die Navigationstasten oder gehen Sie auf den Menüpunkt **Optionen** → **Ändern**.

Gehen Sie folgendermaßen vor, um einen Modus für Anti-Spam zu ändern:

1. Wählen Sie auf der Registerkarte **Anti-Spam** den Punkt **Modus**.

   Das Fenster **Modus** wird geöffnet.

2. Wählen Sie dazu einen Wert für **Anti-Spam-Modus** (s. Abb. unten).

Abbildung 24. Anti-Spam-Modus ändern

3. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

SCHWARZE LISTE ANLEGEN

Sie können eine Schwarze Liste anlegen, nach der Anti-Spam eingehende SMS-Nachrichten und Anrufe blockieren soll.

Die Liste enthält Telefonnummem und Phrasen, deren Vorhandensein in einer SMS-Nachricht darauf hindeutet, dass es sich um Spam handelt.

Informationen über blockierte SMS-Nachrichten und Anrufe werden in einem Bericht erfasst (s. Abschnitt "Programmberichte" auf S. 103).

IN DIESEM ABSCHNITT

Eintrag zur Schwarzen Liste hinzufügen 54

Eintrag der Schwarzen Liste ändern 56

Eintrag aus Schwarzer Liste löschen 57

Alle Einträge löschen 57

EINTRAG ZUR SCHWARZEN LISTE HINZUFÜGEN

Beachten Sie, dass eine Nummer nicht gleichzeitig auf der Schwarzen und der Weißen Liste der Telefonnummern für Anti-Spam stehen kann. Wenn eine Nummer bereits in einer der Listen vorhanden ist, zeigt Kaspersky Mobile Security 9.0 eine entsprechende Meldung an.

Um die Parameterwerte zu ändern, verwenden Sie den Joystick oder die Navigationstasten oder gehen Sie auf den Menüpunkt **Optionen → Ändern**.

Um der Schwarzen Liste für Anti-Spam einen Eintrag hinzuzufügen:

1. Wählen Sie auf der Registerkarte **Anti-Spam** den Punkt **Schwarze Liste**.

   Das Fenster **Schwarze Liste** wird geöffnet.

2. Gehen Sie auf **Optionen → Eintrag hinzufügen** (s. Abb. unten).

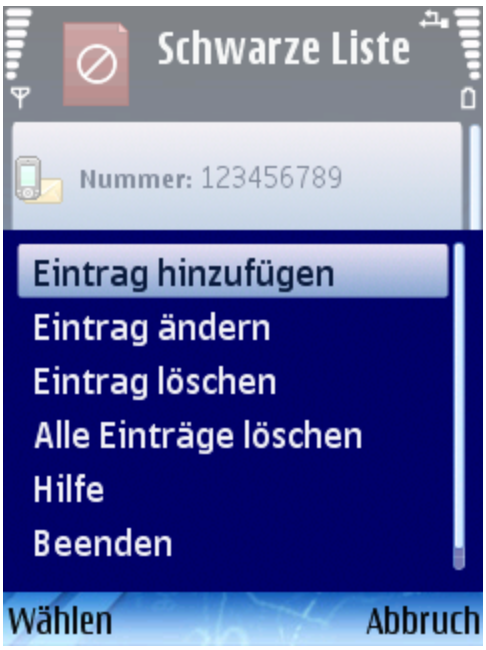


Abbildung 25. Eintrag zur Schwarzen Liste hinzufügen

3. Nehmen Sie folgende Einstellungen vor (s. Abb. unten):

   - **Eingehende blockieren** – Typ der eingehenden Informationen, der von Anti-Spam für eine Nummer blockiert werden soll:
     - **Anrufe und SMS** – eingehende SMS-Nachrichten und Anrufe blockieren
     - **Nur Anrufe** – nur eingehende Anrufe blockieren
     - **Nur SMS** - nur eingehende SMS-Nachrichten blockieren
   - **Von Telefonnummer** – Telefonnummer, von der SMS-Nachrichten und / oder Anrufe blockiert werden. Die Nummer kann mit einer Ziffer, mit einem Buchstaben oder mit dem Zeichen "+" beginnen und darf Ziffern / Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "*" und "?" möglich (wobei "*" für eine beliebige Zeichenfolge steht und "?" für ein beliebiges Einzelzeichen).

- **Mit Text** – Schlüsselwörter / Phrasen, die darauf hinweisen, dass es sich bei einer empfangenen SMS-Nachricht um Spam handelt. Diese Option ist nur verfügbar, wenn der Parameter **Eingehende blockieren** den Wert **Nur SMS** besitzt.

Abbildung 26. Parameter eines Eintrags

4. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

EINTRAG DER SCHWARZEN LISTE ÄNDERN

Für die Einträge aus der Schwarzen Liste der verbotenen Nummern können alle Parameterwerte geändert werden.

Um die Parameterwerte zu ändern, verwenden Sie den Joystick oder die Navigationstasten oder gehen Sie auf den Menüpunkt **Optionen → Ändern**.

Um einen Eintrag in der Schwarzen Liste für Anti-Spam zu ändern:

1. Wählen Sie auf der Registerkarte **Anti-Spam** den Punkt **Schwarze Liste**.

   Das Fenster **Schwarze Liste** wird geöffnet.

2. Markieren Sie in der Liste den Eintrag, den Sie ändern möchten, und gehen Sie dann auf **Optionen → Eintrag ändern**.

3. Nehmen Sie die entsprechenden Einstellungen vor:

   - **Eingehende blockieren** – Typ der eingehenden Informationen, der von Anti-Spam für eine Nummer blockiert werden soll:
     - **Anrufe und SMS** – eingehende SMS-Nachrichten und Anrufe blockieren.
     - **Nur Anrufe** – nur eingehende Anrufe blockieren.
     - **Nur SMS** - nur eingehende SMS-Nachrichten blockieren.
   - **Von Telefonnummer** – Telefonnummer, von der SMS-Nachrichten und / oder Anrufe blockiert werden. Die Nummer kann mit einer Ziffer, mit einem Buchstaben oder mit dem Zeichen "+" beginnen und darf

Ziffern / Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "*" und "?" möglich (wobei "*" für eine beliebige Zeichenfolge steht und "?" für ein beliebiges Einzelzeichen).

- **Mit Text** – Schlüsselwörter / Phrasen, die darauf hinweisen, dass es sich bei einer empfangenen SMS-Nachricht um Spam handelt. Diese Option ist nur verfügbar, wenn der Parameter **Eingehende blockieren** den Wert **Nur SMS** besitzt.

4. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

EINTRAG AUS SCHWARZER LISTE LÖSCHEN

Es kann vorkommen, dass eine Nummer versehentlich zur Schwarzen Liste der verbotenen Nummern hinzugefügt wird. Eine solche Nummer kann aus der Liste gelöscht werden.

Um einen Eintrag aus der Schwarzen Liste für Anti-Spam zu löschen:

1. Wählen Sie auf der Registerkarte **Anti-Spam** den Punkt **Schwarze Liste**.

   Das Fenster **Schwarze Liste** wird geöffnet.

2. Markieren Sie in der Liste den Eintrag, den Sie löschen möchten, und gehen Sie dann auf **Optionen → Eintrag löschen**.

ALLE EINTRÄGE LÖSCHEN

Um alle Einträge aus der Schwarzen Liste für Anti-Spam zu löschen:

1. Wählen Sie auf der Registerkarte **Anti-Spam** den Punkt **Schwarze Liste**.

   Das Fenster **Schwarze Liste** wird geöffnet.

2. Gehen Sie auf **Optionen → Alle Einträge löschen**.

Die Liste wird geleert.

WEISSE LISTE ANLEGEN

Sie können eine Weiße Liste anlegen, nach der Anti-Spam eingehende SMS-Nachrichten und Anrufe erlauben soll.

Die Liste enthält Telefonnummern von Absendern und Phrasen, von denen kein Spam erwartet wird.

IN DIESEM ABSCHNITT

Eintrag zur Weißen Liste hinzufügen 58

Eintrag der Weißen Liste ändern 59

Eintrag aus Weißer Liste löschen 60

Alle Einträge aus Weißer Liste löschen 60

EINTRAG ZUR WEISSEN LISTE HINZUFÜGEN

Beachten Sie, dass eine Nummer nicht gleichzeitig auf der Schwarzen und Weißen Liste der Telefonnummern für Anti-Spam stehen kann. Wenn eine Nummer bereits in einer der Listen vorhanden ist, zeigt Kaspersky Mobile Security 9.0 eine entsprechende Meldung an.

Um die Parameterwerte zu ändern, verwenden Sie den Joystick oder die Navigationstasten oder gehen Sie auf den Menüpunkt **Optionen** → **Ändern**.

Um der Weißen Liste für Anti-Spam einen Eintrag hinzuzufügen:

1. Wählen Sie auf der Registerkarte **Anti-Spam** den Punkt **Weiße Liste**.

   Das Fenster **Weiße Liste** wird geöffnet.

2. Gehen Sie auf **Optionen** → **Eintrag hinzufügen** (s. Abb. unten).

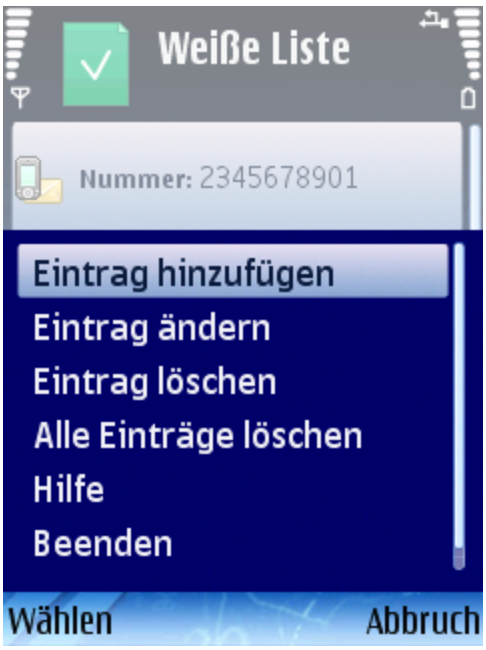


Abbildung 27. Eintrag zur Weißen Liste hinzufügen

3. Legen Sie folgende Parameter für den neuen Eintrag fest (s. Abb. unten):

   - **Eingehende erlauben** – Typ der eingehenden Informationen, der von Anti-Spam für eine Nummer erlaubt werden soll:
     - **Anrufe und SMS** – eingehende Anrufe und SMS-Nachrichten erlauben
     - **Nur Anrufe** – nur eingehende Anrufe erlauben
     - **Nur SMS** - nur eingehende SMS-Nachrichten erlauben
   - **Von Telefonnummer** – Telefonnummer, für die der Empfang von SMS-Nachrichten und / oder Anrufen erlaubt werden soll. Die Nummer kann mit einer Ziffer, mit einem Buchstaben oder mit dem Zeichen "+" beginnen und darf Ziffern / Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "*" und "?" möglich (wobei "*" für eine beliebige Zeichenfolge steht, "?" für ein beliebiges Einzelzeichen).

- **Mit Text** – Schlüsselwörter/Phrasen, die darauf hinweisen, dass es sich bei einer empfangenen SMS-Nachricht nicht um Spam handelt. Diese Option ist nur verfügbar, wenn der Parameter **Eingehende erlauben** den Wert **Nur SMS** besitzt.

Abbildung 28. Parameter eines Eintrags

4. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

EINTRAG DER WEISSEN LISTE ÄNDERN

Alle Parameterwerte der Einträge aus der Weißen Liste für erlaubte Nummern können geändert werden.

Um die Parameterwerte zu ändern, verwenden Sie den Joystick oder die Navigationstasten oder gehen Sie auf den Menüpunkt **Optionen → Ändern**.

➧ *Um einen Eintrag in der Weißen Liste für Anti-Spam zu ändern:*

1. Wählen Sie auf der Registerkarte **Anti-Spam** den Punkt **Weiße Liste**.

   Das Fenster **Weiße Liste** wird geöffnet.

2. Markieren Sie in der Liste den Eintrag, den Sie ändern möchten, und gehen Sie dann auf **Optionen → Eintrag ändern**.

3. Passen Sie den Eintrag entsprechend an:

   - **Eingehende erlauben** – Typ der eingehenden Informationen, der von Anti-Spam für eine Nummer erlaubt werden soll:
     - **Anrufe und SMS** – eingehende Anrufe und SMS-Nachrichten erlauben.
     - **Nur Anrufe** – nur eingehende Anrufe erlauben.
     - **Nur SMS** - nur eingehende SMS-Nachrichten erlauben.
   - **Von Telefonnummer** – Telefonnummer, für die der Empfang von SMS-Nachrichten und / oder Anrufen erlaubt werden soll. Die Nummer kann mit einer Ziffer, mit einem Buchstaben oder mit dem Zeichen "+"

beginnen und darf Ziffern / Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "*" und "?" möglich (wobei "*" für eine beliebige Zeichenfolge steht, "?" für ein beliebiges Einzelzeichen).

- **Mit Text** – Schlüsselwörter/Phrasen, die darauf hinweisen, dass es sich bei einer empfangenen SMS-Nachricht nicht um Spam handelt. Diese Option ist nur verfügbar, wenn der Parameter **Eingehende erlauben** den Wert **Nur SMS** besitzt.

4. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

EINTRAG AUS WEIßER LISTE LÖSCHEN

Um einen Eintrag aus der Weißen Liste für Anti-Spam zu löschen:

1. Wählen Sie auf der Registerkarte **Anti-Spam** den Punkt **Weiße Liste**.

   Das Fenster **Weiße Liste** wird geöffnet.

2. Markieren Sie in der Liste den Eintrag, den Sie löschen möchten, und gehen Sie dann auf **Optionen → Eintrag löschen**.

ALLE EINTRÄGE AUS WEIßER LISTE LÖSCHEN

Um alle Einträge aus der Weißen Liste für Anti-Spam zu löschen:

1. Wählen Sie auf der Registerkarte **Anti-Spam** den Punkt **Weiße Liste**.

   Das Fenster **Weiße Liste** wird geöffnet.

2. Gehen Sie auf **Optionen → Alle Einträge löschen**.

REAKTION AUF SMS-NACHRICHTEN UND ANRUFE VON KONTAKTEN, DIE NICHT IM TELEFONBUCH STEHEN

Im Modus **Beide Listen** oder **Weiße Liste** (s. Abschnitt "Über die Modi für Anti-Spam" auf S. 141) können Sie zusätzlich festlegen, wie Anti-Spam auf SMS-Nachrichten und Anrufe von Nummern reagieren soll, die sich nicht in den Kontakten befinden. Die Weiße Liste von Anti-Spam lässt sich durch Aufnahme der Nummern aus den Kontakten erweitern.

Um die Parameterwerte zu ändern, verwenden Sie den Joystick oder die Navigationstasten des Geräts oder gehen Sie auf **Optionen → Ändern**.

Gehen Sie folgendermaßen vor, um festzulegen, wie Anti-Spam auf eine Nummer reagieren soll, die nicht im Telefonbuch des Geräts steht:

1. Wählen Sie auf der Registerkarte **Anti-Spam** den Punkt **Modus**.

   Das Fenster **Modus** wird geöffnet.

2. Wählen Sie einen Wert für **Kontakte erlauben** (s. Abb. unten):

   - Wählen Sie **Ja**, damit Anti-Spam das Telefonbuch des Geräts als zusätzliche Weiße Liste verwendet.

- Wählen Sie den Wert **Nein**, damit SMS-Nachrichten und Anrufe nur nach dem festgelegten Anti-Spam-Modus gefiltert werden.

Abbildung 29. Reaktion von Anti-Spam auf Nummern, die nicht im Telefonbuch des Geräts stehen

3. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

REAKTION AUF SMS-NACHRICHTEN VON NICHT-ZIFFERN-NUMMERN

Im Modus **Beide Listen** oder **Schwarze Liste** (s. Abschnitt "Über die Modi für Anti-Spam" auf S. 141) können Sie die Schwarze Liste durch Aufnahme aller Nicht-Ziffern-Nummern (Nummern, die Buchstaben enthalten) erweitern. In diesem Fall blockiert Anti-Spam den Empfang von SMS-Nachrichten, die von Nicht-Ziffern-Nummern stammen.

Um die Parameterwerte zu ändern, verwenden Sie den Joystick oder die Navigationstasten des Geräts oder gehen Sie auf **Optionen → Ändern**.

Gehen Sie folgendermaßen vor, um festzulegen, wie Anti-Spam auf eingehende SMS-Nachrichten von Nicht-Ziffern-Nummern reagieren soll:

1. Wählen Sie auf der Registerkarte **Anti-Spam** den Punkt **Modus**.

   Das Fenster **Modus** wird geöffnet.

2. Wählen Sie einen Wert für den Parameter **Nicht-Ziffern-Nummern** (s. Abb. unten):

   - Wählen Sie den Wert **Blockieren**, damit Anti-Spam SMS-Nachrichten von Nicht-Ziffern-Nummern automatisch löscht.

- Wählen Sie den Wert **Erlauben**, damit Anti-Spam Nachrichten von Nicht-Ziffern-Nummern nur auf Basis des gewählten Anti-Spam-Modus filtert.

Abbildung 30. Aktion von Anti-Spam für eingehende SMS-Nachrichten von Nicht-Ziffern-Nummern anpassen

3. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

AKTION FÜR EINGEHENDE SMS-NACHRICHTEN WÄHLEN

Als Standardmodus für Anti-Spam gilt **Beide Listen** (s. Abschnitt "Über die Modi für Anti-Spam" auf S. 141). Anti-Spam prüft eingehende SMS-Nachrichten auf Übereinstimmungen mit der Schwarzen und Weißen Liste.

Wenn die Nummer des Absenders auf keiner der beiden Listen steht, werden Sie von Anti-Spam darüber informiert und nach einer Aktion für die eingehende SMS gefragt.

Sie können eine der folgenden Aktionen für eine SMS-Nachricht wählen (s. Abb. unten):

- Um eine SMS-Nachricht zu blockieren und die Telefonnummer des Absenders in die Schwarze Liste aufzunehmen, wählen Sie **Optionen → Zur Schwarzen Liste**.

- Um eine SMS-Nachricht zu erlauben und die Telefonnummer des Absenders in die Weiße Liste aufzunehmen, wählen Sie **Optionen → Zur Weißen Liste**.

- Um eine SMS-Nachricht zu erlauben und die Telefonnummer des Absenders in keine der Listen einzutragen, wählen Sie **Überspringen**.

Abbildung 31. Meldung von Anti-Spam über den Empfang einer SMS-Nachricht

Informationen über blockierte Nachrichten werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. 103).

AKTION FÜR EINGEHENDE ANRUFE WÄHLEN

Als Standardmodus für Anti-Spam gilt **Beide Listen** (s. Abschnitt "Über die Modi für Anti-Spam" auf S. 141). Anti-Spam prüft eingehende Anrufe auf Übereinstimmungen mit der Schwarzen und Weißen Liste.

Wenn die Nummer des Absenders auf keiner der beiden Listen steht, werden Sie von Anti-Spam nach Gesprächsende darüber informiert und nach einer Aktion für den eingehenden Anruf gefragt.

Für eine Nummer, von der ein Anruf erfolgte, können Sie eine der folgenden Aktionen wählen (s. Abb. unten):

- Um die Telefonnummer des Anrufers in die Schwarze Liste aufzunehmen, wählen Sie **Optionen → Zur Schwarzen Liste**.

- Um die Telefonnummer des Anrufers in die Weiße Liste aufzunehmen, wählen Sie **Optionen → Zur Weißen Liste**.

- Damit die Telefonnummer des Anrufers in keine der Listen eingetragen wird, wählen Sie **Überspringen**.

Abbildung 32. Meldung von Anti-Spam über einen angenommenen Anruf

Informationen über blockierte Anrufe werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. 103).

AUSGEHENDE ANRUFE UND SMS-NACHRICHTEN EINSCHRÄNKEN

Dieser Abschnitt informiert über die Komponente *Kindersicherung,* mit der ausgehende Anrufe und SMS-Nachrichten an bestimmte Nummern eingeschränkt werden können. Außerdem werden hier folgende Vorgänge beschrieben: Liste für erlaubte und verbotene Nummern anlegen, Kindersicherung anpassen.

IN DIESEM ABSCHNITT

Kindersicherung....64

Modi der Kindersicherung....65

Modus für die Kindersicherung ändern....65

Schwarze Liste anlegen....66

Weiße Liste anlegen....69

KINDERSICHERUNG

Die Komponente *Kindersicherung* filtert ausgehende SMS-Nachrichten und Anrufe nach einer Schwarzen und Weißen Nummernliste.

Wird mindestens eine Übereinstimmung festgestellt, so erfolgt keine weitere Untersuchung. Eine ausgehende SMS-Nachricht oder ein ausgehender Anruf, die/der einem Element der Schwarzen Liste entspricht, wird gesperrt. Bei einer Übereinstimmung mit der Weißen Liste wird der Vorgang erlaubt.

Die Kindersicherung sperrt nur SMS-Nachrichten, die mit Hilfe der Standardmittel des Geräts gesendet werden. Das Blockieren erstreckt sich nicht auf SMS-Nachrichten, die mit Programmen von Drittherstellern gesendet werden.

Informationen über die Arbeit der Komponente werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. 103).

MODI DER KINDERSICHERUNG

Die Kindersicherung schützt Ihr Gerät vor unerwünschten ausgehenden SMS-Nachrichten und Anrufen.

Es sind die folgenden Optionen für die Kindersicherung vorgesehen:

- **Aus** – Kindersicherung deaktivieren. Ausgehende SMS-Nachrichten und Anrufe werden nicht gefiltert.

  Dieser Modus gilt als Standard.

- **Schwarze Liste** – Das Senden von SMS-Nachrichten / Anrufen wird nur an Nummern aus der Schwarzen Liste verboten. Alle übrigen Nachrichten und Anrufe werden erlaubt.

- **Weiße Liste** – Das Senden von SMS-Nachrichten / Anrufen wird nur an Nummern aus der Weißen Liste erlaubt. Alle übrigen Nachrichten und Anrufe werden blockiert.

Sie können den Modus der Kindersicherung ändern (s. Abschnitt "Modus der Kindersicherung ändern" auf S. 65).

Der aktuelle Modus der Kindersicherung wird auf der Registerkarte **Kindersicherung** neben dem Menüpunkt **Modus** angezeigt.

MODUS FÜR DIE KINDERSICHERUNG ÄNDERN

Um die Parameterwerte zu ändern, verwenden Sie den Joystick oder die Navigationstasten oder gehen Sie auf den Menüpunkt **Optionen** → **Ändern**.

Gehen Sie folgendermaßen vor, um einen Modus für die Kindersicherung zu ändern:

1. Wählen Sie auf der Registerkarte **Kindersicherung** gehen Sie auf den Punkt **Modus**.

   Das Fenster **Modus** wird geöffnet.

2. Wählen Sie einen Modus für die Kindersicherung (s. Abb. unten).

Abbildung 33. Modus für die Kindersicherung ändern

3. Klicken Sie auf **OK**, um die Änderungen zu speichern.

SCHWARZE LISTE ANLEGEN

Sie können eine Schwarze Liste anlegen, nach der die Kindersicherung ausgehende SMS-Nachrichten und Anrufe blockieren soll. Die Liste enthält Telefonnummern, an die ausgehende SMS-Nachrichten und Anrufe verboten werden.

Informationen über blockierte SMS-Nachrichten und Anrufe werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. 103).

IN DIESEM ABSCHNITT

Eintrag zur Schwarzen Liste hinzufügen 66

Eintrag der Schwarzen Liste ändern 68

Eintrag aus Schwarzer Liste löschen 69

Alle Einträge aus Schwarzer Liste löschen 69

EINTRAG ZUR SCHWARZEN LISTE HINZUFÜGEN

Beachten Sie, dass eine Nummer nicht gleichzeitig auf der Schwarzen und Weißen Nummernliste der Kindersicherung stehen kann. Wenn eine Nummer bereits in einer der Listen vorhanden ist, zeigt Kaspersky Mobile Security 9.0 eine entsprechende Meldung an.

Um die Parameterwerte zu ändern, verwenden Sie den Joystick oder die Navigationstastenoder gehen Sie auf den Menüpunkt **Optionen → Ändern**.

Um der Schwarzen Liste der Kindersicherung einen Eintrag hinzuzufügen:

1. Wählen Sie auf der Registerkarte **Kindersicherung** den Punkt **Schwarze Liste**.

   Das Fenster **Schwarze Liste** wird geöffnet.

2. Gehen Sie auf **Optionen** → **Eintrag hinzufügen** (s. Abb. unten).

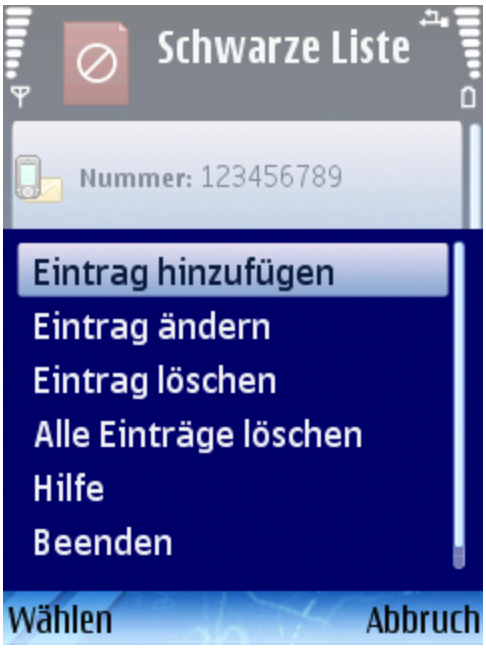


Abbildung 34. Eintrag zur Schwarzen Liste hinzufügen

3. Legen Sie folgende Parameter für den neuen Eintrag fest (s. Abb. unten):

   - **Ausgehende verbieten** – Typ der ausgehenden Informationen, der von der Kindersicherung für eine Nummer blockiert werden soll:

     - **Anrufe und SMS** – ausgehende SMS-Nachrichten und Anrufe blockieren.
     - **Nur Anrufe** – nur ausgehende Anrufe blockieren.
     - **Nur SMS** - nur ausgehende SMS-Nachrichten blockieren.

- **An Telefonnummer** – Telefonnummer, an die ausgehende SMS-Nachrichten und/oder Anrufe blockiert werden sollen. Die Nummer kann mit einer Ziffer, mit einem Buchstaben oder mit dem Zeichen "+" beginnen und darf Ziffern / Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "*" und "?" möglich (wobei "*" für eine beliebige Zeichenfolge steht und "?" für ein beliebiges Einzelzeichen).

Abbildung 35. Parameter eines Eintrags

4. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

EINTRAG DER SCHWARZEN LISTE ÄNDERN

Für die Einträge aus der Schwarzen Liste der verbotenen Nummern können alle Parameterwerte geändert werden.

Um die Parameterwerte zu ändern, verwenden Sie den Joystick oder die Navigationstasten oder gehen Sie auf den Menüpunkt **Optionen → Ändern**.

➧ *Um einen Eintrag in der Schwarzen Liste der Kindersicherung zu ändern:*

1. Wählen Sie auf der Registerkarte **Kindersicherung** den Punkt **Schwarze Liste**.

   Das Fenster **Schwarze Liste** wird geöffnet.

2. Markieren Sie in der Liste den Eintrag, den Sie ändern möchten, und gehen Sie dann auf **Optionen → Einträg ändern**.

3. Nehmen Sie die entsprechenden Einstellungen vor:

   - **Ausgehende verbieten** – Typ der ausgehenden Informationen, der von der Kindersicherung für eine Nummer blockiert werden soll:
     - **Anrufe und SMS** – ausgehende SMS-Nachrichten und Anrufe blockieren
     - **Nur Anrufe** – nur ausgehende Anrufe blockieren
     - **Nur SMS** - nur ausgehende SMS-Nachrichten blockieren
   - **An Telefonnummer** – Telefonnummer, an die ausgehende SMS-Nachrichten und/oder Anrufe blockiert werden sollen. Die Nummer kann mit einer Ziffer, mit einem Buchstaben oder mit dem Zeichen "+"

beginnen und darf Ziffern / Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "*" und "?" möglich (wobei "*" für eine beliebige Zeichenfolge steht und "?" für ein beliebiges Einzelzeichen).

4. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

EINTRAG AUS SCHWARZER LISTE LÖSCHEN

Es kann vorkommen, dass eine Nummer versehentlich zur Schwarzen Liste der verbotenen Nummern hinzugefügt wird. Eine solche Nummer kann aus der Liste gelöscht werden.

Um einen Eintrag aus der Schwarzen Liste der Kindersicherung zu löschen:

1. Wählen Sie auf der Registerkarte **Kindersicherung** den Punkt **Schwarze Liste**.

   Das Fenster **Schwarze Liste** wird geöffnet.

2. Markieren Sie in der Liste den Eintrag, den Sie löschen möchten, und gehen Sie dann auf **Optionen → Eintrag löschen**.

ALLE EINTRÄGE AUS SCHWARZER LISTE LÖSCHEN

Um alle Einträge aus der Schwarzen Liste der Kindersicherung zu löschen:

1. Wählen Sie auf der Registerkarte **Kindersicherung** den Punkt **Schwarze Liste**.

   Das Fenster **Schwarze Liste** wird geöffnet.

2. Gehen Sie auf **Optionen → Alle Einträge löschen**.

Die Liste wird geleert.

WEISSE LISTE ANLEGEN

Sie können eine Weiße Liste anlegen, nach der die Kindersicherung ausgehende SMS-Nachrichten und Anrufe erlauben soll.

Die Liste enthält Telefonnummern, an die ausgehende SMS-Nachrichten und Anrufe von der Kindersicherung erlaubt werden.

Informationen über blockierte SMS-Nachrichten und Anrufe werden in einem Programmbericht (s. Abschnitt "Programmberichte" auf S. 103).

IN DIESEM ABSCHNITT

Eintrag hinzufügen 70

Eintrag der Weißen Liste ändern 71

Eintrag aus Weißer Liste löschen 72

Alle Einträge löschen 72

EINTRAG HINZUFÜGEN

Beachten Sie, dass eine Nummer nicht gleichzeitig auf der Schwarzen und Weißen Nummernliste der Kindersicherung stehen kann. Wenn eine Nummer bereits in einer der Listen vorhanden ist, zeigt Kaspersky Mobile Security 9.0 eine entsprechende Meldung an.

Um die Parameterwerte zu ändern, verwenden Sie den Joystick oder die Navigationstasten oder gehen Sie auf den Menüpunkt **Optionen → Ändern**.

Um der Weißen Liste der Kindersicherung einen Eintrag hinzuzufügen:

1. Wählen Sie auf der Registerkarte **Kindersicherung** den Punkt **Weiße Liste**.

   Das Fenster **Weiße Liste** wird geöffnet.

2. Gehen Sie auf **Optionen → Eintrag hinzufügen** (s. Abb. unten).

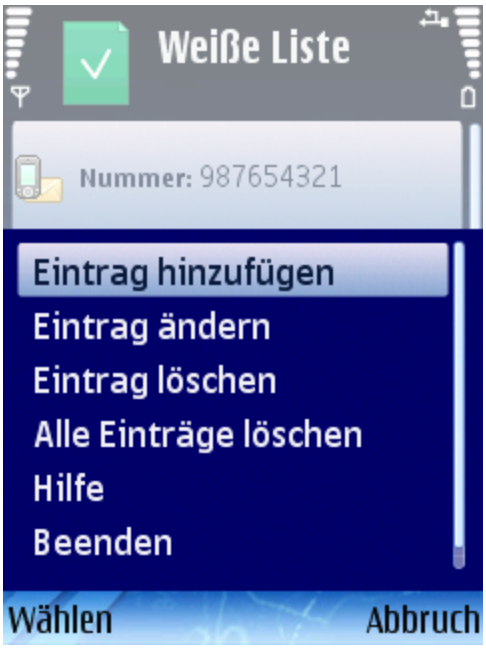


Abbildung 36. Eintrag zur Weißen Liste hinzufügen

3. Legen Sie folgende Parameter für den neuen Eintrag fest (s. Abb. unten):

   - **Ausgehende erlauben** – Typ der ausgehenden Informationen, der von der Kindersicherung für eine Nummer erlaubt werden soll:
     - **Anrufe und SMS** – ausgehende SMS-Nachrichten und Anrufe erlauben
     - **Nur Anrufe** – nur ausgehende Anrufe erlauben
     - **Nur SMS** – nur ausgehende SMS-Nachrichten erlauben

- **An Telefonnummer** – Telefonnummer, an die die Kindersicherung ausgehende SMS-Nachrichten / Anrufe erlauben soll. Die Nummer kann mit einer Ziffer, mit einem Buchstaben oder mit dem Zeichen "+" beginnen und darf Ziffern / Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "*" und "?" möglich (wobei "*" für eine beliebige Zeichenfolge steht, "?" für ein beliebiges Einzelzeichen).

Abbildung 37. Parameter eines Eintrags

4. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

EINTRAG DER WEIßEN LISTE ÄNDERN

Alle Parameterwerte der Einträge aus der Weißen Liste für erlaubte Nummern können geändert werden.

Um die Parameterwerte zu ändern, verwenden Sie den Joystick oder die Navigationstasten oder gehen Sie auf den Menüpunkt **Optionen → Ändern**.

Um einen Eintrag in der Weißen Liste der Kindersicherung zu ändern:

1. Wählen Sie auf der Registerkarte **Kindersicherung** den Punkt **Weiße Liste**.

   Das Fenster **Weiße Liste** wird geöffnet.

2. Markieren Sie in der Liste den Eintrag, den Sie ändern möchten, und gehen Sie dann auf **Optionen → Eintrag ändern**.

3. Nehmen Sie die entsprechenden Einstellungen vor:

   - **Ausgehende erlauben** – Typ der ausgehenden Informationen, der von der Kindersicherung für eine Nummer erlaubt werden soll:

     - **Anrufe und SMS** – ausgehende SMS-Nachrichten und Anrufe erlauben.
     - **Nur Anrufe** – nur ausgehende Anrufe erlauben.
     - **Nur SMS** – nur ausgehende SMS-Nachrichten erlauben.

   - **An Telefonnummer** – Telefonnummer, an die die Kindersicherung ausgehende SMS-Nachrichten / Anrufe erlauben soll. Die Nummer kann mit einer Ziffer, mit einem Buchstaben oder mit dem Zeichen "+" beginnen

und darf Ziffern / Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "*" und "?" möglich (wobei "*" für eine beliebige Zeichenfolge steht, "?" für ein beliebiges Einzelzeichen).

4. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

EINTRAG AUS WEISSER LISTE LÖSCHEN

Es kann vorkommen, dass eine Nummer versehentlich zur Weißen Liste hinzugefügt wurde. Eine Nummer kann aus der erstellten Liste gelöscht werden.

Um einen Eintrag aus der Weißen Liste der Kindersicherung zu löschen:

1. Wählen Sie auf der Registerkarte **Kindersicherung** den Punkt **Weiße Liste**.

   Das Fenster **Weiße Liste** wird geöffnet.

2. Markieren Sie in der Liste den Eintrag, den Sie löschen möchten, und gehen Sie dann auf **Optionen → Eintrag löschen**.

ALLE EINTRÄGE LÖSCHEN

Um alle Einträge aus der Weißen Liste der Kindersicherung zu löschen:

1. Wählen Sie auf der Registerkarte **Kindersicherung** den Punkt **Weiße Liste**.

   Das Fenster **Weiße Liste** wird geöffnet.

2. Gehen Sie auf **Optionen → Alle Einträge löschen**.

Die Liste wird geleert.

DATENSCHUTZ BEI VERLUST ODER DIEBSTAHL DES GERÄTS

Dieser Abschnitt informiert über die Komponente *Diebstahlschutz*, die bei Diebstahl oder Verlust des Geräts einen komplexen Schutz für persönliche Daten bietet und das Auffinden des Geräts erleichtert. Außerdem werden hier folgende Vorgänge beschrieben: Diebstahlschutz aktivieren / deaktivieren, Diebstahlschutz anpassen, Schutz bei Diebstahl oder Verlust des Geräts ferngesteuert starten.

IN DIESEM ABSCHNITT

Diebstahlschutz 73

Gerät blockieren 73

Persönliche Daten löschen 75

Liste der zu löschenden Objekte erstellen 77

Wechsel der SIM-Karte auf dem Gerät überwachen 78

Geografische Koordinaten des Geräts ermitteln 79

Diebstahlschutz-Funktionen ferngesteuert starten 81

DIEBSTAHLSCHUTZ

Der Diebstahlschutz schützt die Daten, die auf dem Gerät gespeichert sind, vor unbefugtem Zugriff. Diese Funktion ist von Vorteil, wenn das Gerät verloren geht oder gestohlen wird. Der Diebstahlschutz erlaubt es, per Fernsteuerung ein Gerät zu blockieren und die darauf gespeicherten Daten zu löschen.

Die Komponente umfasst folgende Funktionen:

- Mit der Funktion **SMS-Block** kann das Gerät auf Befehl des Benutzers blockiert werden, und der Benutzer kann einen Text eingeben, der auf dem Display des blockierten Geräts angezeigt wird.
- Die Funktion **SMS-Clean** ermöglicht es, persönliche Benutzerdaten (alle Kontakte, Nachrichten, Galerie, Kalender, Berichte, Netzwerkeinstellungen) aus dem Gerät sowie Daten von Speicherkarten und Dateien aus bestimmten Ordnern unwiderruflich zu löschen.
- **SIM-Watch** erlaubt es, an eine vorgegebene Telefonnummer und / oder E-Mail-Adresse die neue Telefonnummer zu schicken und das Gerät zu sperren, wenn die SIM-Karte gewechselt oder das Gerät ohne SIM eingeschaltet wird.
- **GPS-Find** kann die geografischen Koordinaten des Geräts ermitteln und diese Daten per SMS an das anfragende Gerät oder an eine vorgegebene E-Mail-Adresse senden.

  Diese Funktion eignet sich nur für Geräte mit integriertem GPS-Empfänger.

Für die Verwendung der einzelnen Diebstahlschutz-Funktionen ist der Geheimcode erforderlich, der beim ersten Start von Kaspersky Mobile Security 9.0 festgelegt wurde.

Alle Diebstahlschutz-Funktionen sind nach der Installation von Kaspersky Mobile Security 9.0 deaktiviert.

Außerdem lassen sich die Diebstahlschutz-Funktionen von Kaspersky Mobile Security 9.0 durch SMS-Befehle an das vermisste / gestohlene Gerät starten (s. Abschnitt "Diebstahlschutz-Funktionen ferngesteuert starten" auf S. 81).

Der aktuelle Status der einzelnen Funktionen wird auf der Registerkarte **Diebstahlschutz** neben der jeweiligen Funktion angezeigt.

Informationen über die Arbeit der Komponente werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. 103).

GERÄT BLOCKIEREN

Wenn das Gerät vermisst wird oder gestohlen wurde, kann der Zugriff auf die im Gerät gespeicherten Daten mit der ferngesteuerten Funktion SMS-Block gesperrt werden. Das Gerät kann nur durch Eingabe des Geheimcodes entsperrt werden.

Diese Funktion blockiert das Gerät nicht, sondern aktiviert eine Option für das ferngesteuerte Blockieren.

Um die Parameterwerte zu ändern, verwenden Sie den Joystick oder die Navigationstastenoder gehen Sie auf den Menüpunkt **Optionen → Ändern**.

Gehen Sie folgendermaßen vor, um die Funktion SMS-Block zu aktivieren:

1. Wählen Sie auf der Registerkarte **Diebstahlschutz** den Punkt **SMS-Block**.

   Das Fenster **SMS-Block** wird geöffnet.

2. Setzen Sie den Parameter **Modus für SMS-Block** auf **An**.

3. Damit auf dem Display des blockierten Geräts ein Text angezeigt wird, wählen Sie den Parameter **Text beim Blockieren** und füllen Sie das Feld **Text eingeben** aus (s. Abb. unten). Wenn das Gerät blockiert wird, erscheint in der Grundeinstellung der Text "Gerät blockiert!" auf dem Display.

   Damit kein Text angezeigt wird, wählen Sie **Text beim Blockieren**, löschen Sie das Feld **Text eingeben** und klicken Sie auf **OK**.

Abbildung 38. Einstellungen der Funktion SMS-Block

4. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

Ein vermisstes Gerät, auf dem die Funktion SMS-Block aktiviert ist, kann auf folgende Weise gesperrt werden:

- Mit der Funktion **Befehl senden**. Dafür ist ein anderes Gerät erforderlich, auf dem Kaspersky Mobile Security 9.0 installiert ist. Auf dem Zweitgerät wird mit Kaspersky Mobile Security 9.0 eine spezielle SMS-Nachricht erstellt und an das verlorene Gerät gesendet. Sie enthält die Telefonnummer des zu blockierenden Geräts und seinen Geheimcode. Der Empfang der speziellen SMS bleibt auf dem zu blockierenden Gerät unbemerkt.

- Mit den Standardfunktionen zum Erstellen einer SMS-Nachricht. Dazu wird auf dem anderen Gerät eine SMS-Nachricht, die aus einem speziellen Text und dem Geheimcode des zu blockierenden Geräts besteht, erstellt und an das verlorene Gerät gesendet.

Gehen Sie folgendermaßen vor, um einen Befehl an das vermisste Gerät zu senden:

1. Wählen Sie auf der Registerkarte **Erweitert** den Punkt **Befehl senden**.

   Ein Fenster zum Senden eines speziellen Befehls wird geöffnet.

2. Klicken Sie auf **Start**.

3. Wählen Sie den Befehlstyp **SMS-Block** und klicken Sie dann auf **Weiter** (s. Abb. unten).

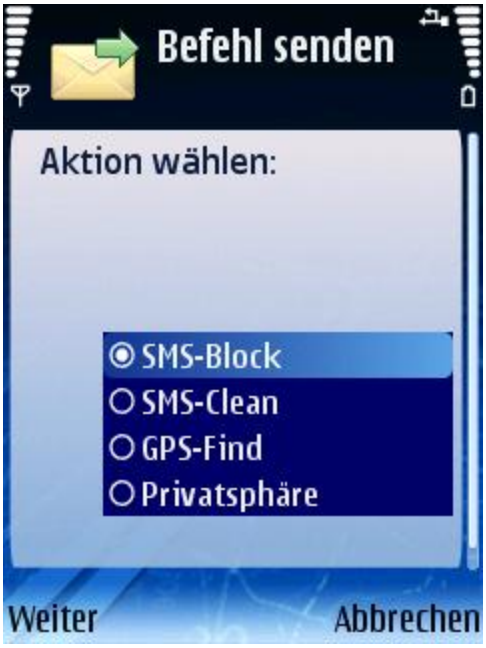


Abbildung 39. Gerät per Fernsteuerung blockieren

4. Tragen Sie die Telefonnummer des Geräts ein, das blockiert werden soll, und klicken Sie dann auf **Weiter**.

5. Tragen Sie den Geheimcode des vermissten Geräts ein und klicken Sie auf **Senden**.

Um mit Hilfe der Standardfunktionen eines Handys eine SMS zu erstellen:

Schicken Sie an das zu blockierende Gerät eine SMS-Nachricht mit dem Text `block:<Code>` (wobei `<Code>` der Geheimcode des zu sperrenden Geräts ist). Die Groß- und Kleinschreibung von Buchstaben und die Leerzeichen vor und nach dem Doppelpunkt sind irrelevant.

PERSÖNLICHE DATEN LÖSCHEN

Bei Diebstahl oder Verlust des mobilen Geräts können mit der Funktion SMS-Clean folgende darauf gespeicherten Informationen gelöscht werden:

- persönliche Benutzerdaten (alle Kontakte, Nachrichten, Galerie, Kalender und Netzwerkeinstellungen). Dabei löscht der Diebstahlschutz die Kontakte, die sich im Telefonbuch des Geräts und auf der SIM-Karte befinden.
- Daten auf Speicherkarten
- Daten im Ordner C:\Data und in anderen festgelegten Ordnern

Das Aktivieren dieser Funktion löscht die auf dem Gerät gespeicherten Daten nicht, sondern aktiviert eine Option zur Datenlöschung.

Der Diebstahlschutz löscht die Daten, die durch die Liste der zu löschenden Objekte festgelegt werden (s. Abschnitt "Liste der zu löschenden Objekte erstellen" auf S. 77) erst dann, wenn das Gerät eine spezielle SMS empfängt.

Gehen Sie folgendermaßen vor, um die Funktion SMS-Clean zu aktivieren:

1. Wählen Sie auf der Registerkarte **Diebstahlschutz** den Punkt **SMS-Clean**.

   Das Fenster **SMS-Clean** wird geöffnet.

2. Gehen Sie auf **Modus**.

   Das Fenster **Modus** wird geöffnet.

3. Gehen Sie auf **Modus für SMS-Clean** und wählen Sie den Wert **An** (s. Abb. unten).

4. Wählen Sie die Daten, die gelöscht werden sollen, wenn das Gerät eine spezielle SMS-Nachricht erhält:

   - Setzen Sie den Parameter **Daten löschen** auf **Ja**, damit persönliche Daten gelöscht werden.
   - Setzen Sie den Parameter **Ordner löschen** auf **Ja**, damit die Dateien aus dem Ordner C:\Data und aus den anderen festgelegten Ordnern gelöscht werden.

Abbildung 40. Einstellungen der Funktion SMS-Clean

5. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

6. Erstellen Sie eine Liste der zu löschenden Ordner (s. Abschnitt "Liste der zu löschenden Objekte erstellen" auf S. 77).

Wenn die Funktion aktiviert ist, können persönliche Daten auf folgende Weise vom Gerät gelöscht werden:

- Befehl an das vermisste / gestohlene Gerät senden mit der Funktion **Befehl senden**. Dafür ist ein anderes Gerät erforderlich, auf dem Kaspersky Mobile Security 9.0 installiert ist. Auf dem Zweitgerät wird mit Kaspersky Mobile Security 9.0 eine spezielle SMS-Nachricht erstellt und an das verlorene Gerät gesendet. Sie enthält die Telefonnummer des Geräts und seinen Geheimcode. Der Empfang einer speziellen SMS bleibt auf dem vermissten / gestohlenen Gerät unbemerkt.

- Mit den Standardfunktionen zum Erstellen einer SMS-Nachricht. Auf dem anderen Gerät wird eine SMS-Nachricht, die aus einem speziellen Text und dem Geheimcode des vermissten/gestohlenen Geräts besteht, erstellt und gesendet.

Gehen Sie folgendermaßen vor, um einen Befehl an das vermisste / gestohlene Gerät zu senden:

1. Wählen Sie auf der Registerkarte **Erweitert** den Punkt **Befehl senden**.

   Ein Fenster zum Senden eines speziellen Befehls wird geöffnet.

2. Klicken Sie auf **Start**.

3. Wählen Sie den Befehlstyp **SMS-Clean** und klicken Sie dann auf **Weiter** (s. Abb. unten).

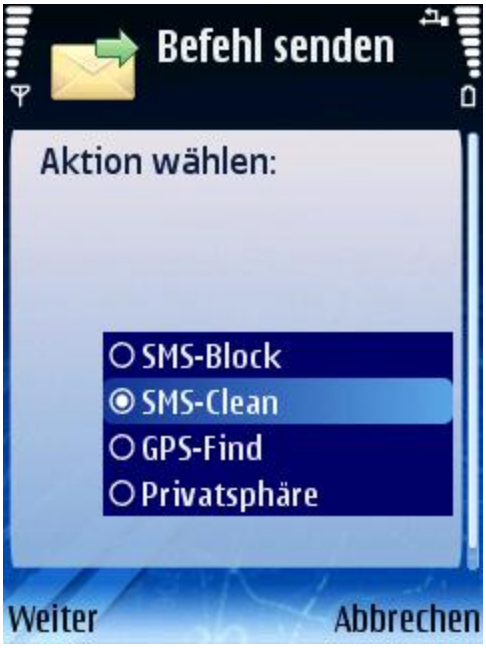


Abbildung 41. Persönliche Daten löschen

4. Tragen Sie die Telefonnummer des Geräts ein, auf dem Daten gelöscht werden sollen, und klicken Sie dann auf **Weiter**.

5. Tragen Sie den Geheimcode des vermissten Geräts ein und klicken Sie auf **Senden**.

Um mit Hilfe der Standardfunktionen eines Handys eine SMS zu erstellen:

Schicken Sie an das vermisste / gestohlene Gerät eine SMS-Nachricht mit dem Text `wipe:<Code>` (wobei `<Code>` der Geheimcode des vermissten Geräts ist). Die Groß- und Kleinschreibung von Buchstaben und die Leerzeichen vor und nach dem Doppelpunkt sind irrelevant.

LISTE DER ZU LÖSCHENDEN OBJEKTE ERSTELLEN

Gehen Sie folgendermaßen vor, um einen Ordner zur Liste der zu löschenden Ordner hinzuzufügen:

1. Wählen Sie auf der Registerkarte **Diebstahlschutz** den Punkt **SMS-Clean**.

   Das Fenster **SMS-Clean** wird geöffnet.

2. Gehen Sie auf **Zu lösch. Ordner**.

   Das Fenster **Zu löschende Ordner** wird geöffnet.

3. Gehen Sie auf **Optionen → Ordner hinzufügen** (s. Abb. unten).

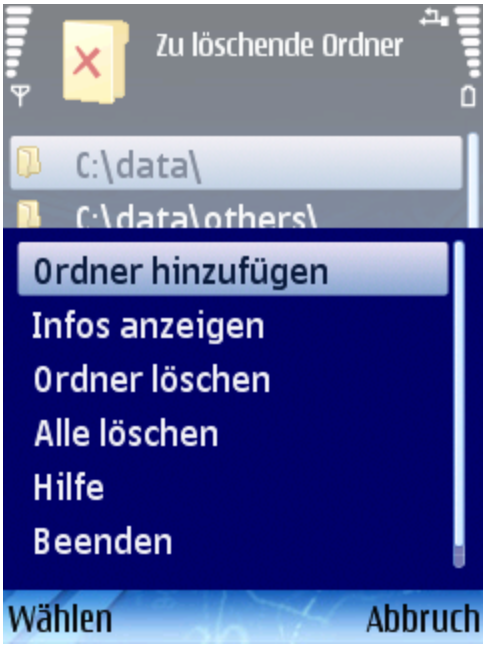


Abbildung 42. Ordner hinzufügen

4. Wählen Sie den entsprechenden Ordner und klicken Sie auf **OK**.

   Der Ordner wird zur Liste hinzugefügt.

5. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

➧ *Gehen Sie folgendermaßen vor, um einen Ordner aus der Liste zu löschen:*

1. Wählen Sie auf der Registerkarte **Diebstahlschutz** den Punkt **SMS-Clean**.

   Das Fenster **SMS-Clean** wird geöffnet.

2. Gehen Sie auf **Zu lösch. Ordner**.

   Das Fenster **Zu löschende Ordner** wird geöffnet.

3. Wählen Sie einen Ordner aus der Liste und gehen Sie auf **Optionen → Ordner löschen**.

4. Bestätigen Sie die Deinstallation mit **Ja**.

WECHSEL DER SIM-KARTE AUF DEM GERÄT ÜBERWACHEN

Wenn die SIM-Karte auf dem verlorenen oder gestohlenen Gerät ausgetauscht wird, schickt SIM-Watch die neue Nummer der eingelegten SIM-Karte an eine vorgegebene Telefonnummer und / oder E-Mail-Adresse und blockiert das Gerät.

➧ *Gehen Sie folgendermaßen vor, um die Funktion SIM-Watch zu aktivieren und den Wechsel der SIM-Karte auf dem Gerät zu kontrollieren:*

1. Wählen Sie auf der Registerkarte **Diebstahlschutz** den Punkt **SIM-Watch**.

   Das Fenster **SIM-Watch** wird geöffnet.

2. Setzen Sie **Modus für SIM-Watch** auf **An**.

3. Legen Sie folgende Parameter für SIM-Watch fest (s. Abb. unten):

   - **E-Mail-Adresse**. Wenn Sie per E-Mail über die neue Nummer Ihres Telefons informiert werden möchten, geben Sie eine E-Mail-Adresse an.

   - **Telefonnummer**. Um automatisch eine Nachricht über die neue Nummer Ihres Telefons zu erhalten, geben Sie die Telefonnummer an, an die eine Nachricht geschickt werden soll. Die Nummer kann mit einer Ziffer oder dem Zeichen "+" beginnen und darf nur Ziffern enthalten.

   - **Bei Wechsel der SIM-Karte**. Damit das Gerät beim Wechsel der SIM-Karte oder beim Einschalten ohne Karte blockiert wird, wählen Sie den Wert **Blockieren**. Das Gerät kann durch Eingabe des Geheimcodes entsperrt werden. Das Blockieren des Geräts ist standardmäßig deaktiviert.

   - **Text beim Blockieren**. Damit auf dem Display des blockierten Geräts eine Nachricht erscheint, füllen Sie das Feld **Text eingeben** aus. In der Grundeinstellung wird der Text "Gerät blockiert" auf dem Display angezeigt.

Abbildung 43. Einstellungen die Funktion SIM-Watch

4. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

GEOGRAFISCHE KOORDINATEN DES GERÄTS ERMITTELN

Die Funktion GPS-Find ermittelt die geografischen Koordinaten des Geräts und schickt sie mit einer SMS oder E-Mail an das anfragende Gerät oder an eine vorgegebene E-Mail-Adresse.

Diese Funktion eignet sich nur für Geräte mit integriertem GPS-Empfänger. Der GPS-Empfänger wird bei Bedarf automatisch aktiviert.

Eine Ortung ist nur möglich, wenn sich das Gerät im Empfangsbereich von Satelliten befindet. Besteht im Augenblick der Anfrage kein Satellitenempfang, dann wird in regelmäßigen Abständen versucht, eine Verbindung herzustellen.

➡ *Gehen Sie folgendermaßen vor, um GPS-Find zu aktivieren:*

1. Wählen Sie auf der Registerkarte **Diebstahlschutz** den Punkt **GPS-Find**.

   Das Fenster **GPS-Find** wird geöffnet.

2. Wählen Sie für **Modus für GPS-Find** den Wert **An**.

3. Legen Sie unter **E-Mail-Adresse** fest, an welche E-Mail-Adresse die Gerätekoordinaten geschickt werden sollen (s. Abb. unten).

Abbildung 44. Einstellungen der Funktion GPS-Find

4. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

Wenn GPS-Find aktiviert ist, können die Koordinaten des Geräts auf folgende Weise ermittelt werden:

- Mit der Funktion **Befehl senden**. Dafür ist ein anderes Gerät erforderlich, auf dem Kaspersky Mobile Security 9.0 installiert ist. Auf dem Zweitgerät wird mit Kaspersky Mobile Security 9.0 eine spezielle SMS-Nachricht erstellt und an das verlorene Gerät gesendet. Sie enthält die Telefonnummer des Geräts und seinen Geheimcode. Der Empfang einer speziellen SMS bleibt auf dem vermissten / gestohlenen Gerät unbemerkt.

- Mit den Standardfunktionen eines Handys, die zum Erstellen einer SMS-Nachricht dienen. Auf dem anderen Gerät wird eine SMS-Nachricht, die aus einem speziellen Text und dem Geheimcode des vermissten/gestohlenen Geräts besteht, erstellt und gesendet.

Gehen Sie folgendermaßen vor, um einen Befehl an das vermisste / gestohlene Gerät zu senden:

1. Wählen Sie auf der Registerkarte **Erweitert** den Punkt **Befehl senden**.

   Ein Fenster zum Senden eines speziellen Befehls wird geöffnet.

2. Wählen Sie den Befehlstyp **GPS-Find** und klicken Sie auf **Weiter** (s. Abb. unten).

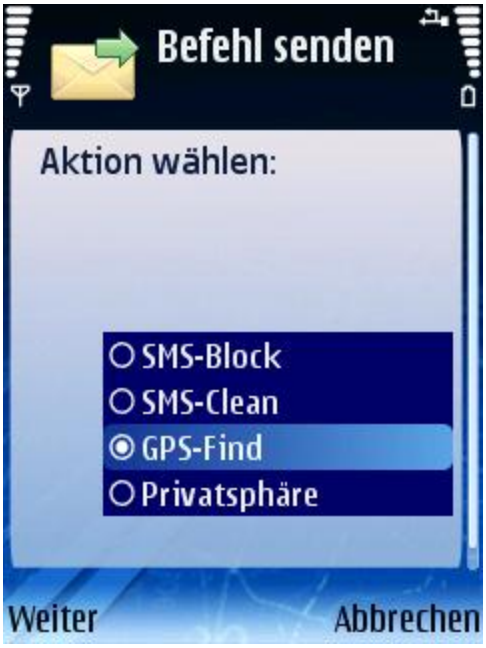


Abbildung 45. Gerät orten

3. Tragen Sie die Telefonnummer des Geräts ein, das Sie orten möchten, und klicken Sie dann auf **Weiter**.

4. Tragen Sie den Geheimcode des vermissten Geräts ein und klicken Sie auf **Senden**.

Um mit Hilfe der Standardfunktionen eines Handys eine SMS zu erstellen:

Schicken Sie an das vermisste / gestohlene Gerät eine SMS-Nachricht mit dem Text `find:<Code>` (wobei `<Code>` der Geheimcode des vermissten Geräts ist). Die Groß- und Kleinschreibung von Buchstaben und die Leerzeichen vor und nach dem Doppelpunkt sind irrelevant.

Eine SMS-Nachricht mit den Koordinaten des Geräts wird an die Nummer gesendet, von der die Ortungsanfrage stammt, sowie an die E-Mail-Adresse, falls diese in den Einstellungen für GPS-Find angegeben wurde.

DIEBSTAHLSCHUTZ-FUNKTIONEN FERNGESTEUERT STARTEN

Mit einer speziellen SMS können Sie einen Befehl senden, um auf einem vermissten / gestohlenen Gerät, auf dem Kaspersky Mobile Security installiert ist, die Diebstahlschutz-Funktionen ferngesteuert zu starten. Der Empfang des Befehls bleibt auf dem zu blockierenden Gerät unbemerkt.

Gehen Sie folgendermaßen vor, um einen Befehl an das vermisste / gestohlene Gerät zu senden:

1. Wählen Sie auf der Registerkarte **Erweitert** den Punkt **Befehl senden**.

   Ein Fenster zum Senden eines speziellen Befehls wird geöffnet.

2. Klicken Sie auf **Start**.

3. Wählen Sie eine Funktion, die per Fernsteuerung gestartet werden soll (s. Abb. unten):

   - **SMS-Block** (s. Abschnitt "Gerät blockieren" auf S. 73).
   - **SMS-Clean** (s. Abschnitt "Persönliche Daten löschen" auf S. 75).

- **GPS-Find** (s. Abschnitt "Geografische Koordinaten des Geräts ermitteln" auf S. 79).
- **Privatsphäre** (s. Abschnitt "Über die Privatsphäre" auf S. 83).

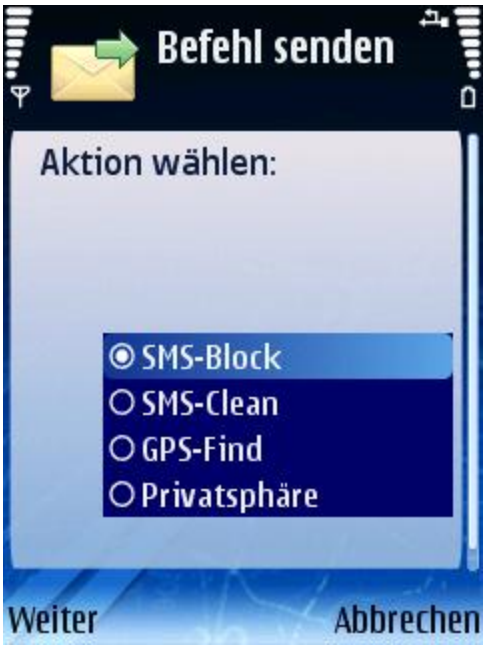


Abbildung 46. Diebstahlschutz-Funktionen ferngesteuert starten

Die betreffende Funktion muss auf dem Gerät, das die Nachricht empfangen soll, aktiviert sein.

4. Klicken Sie auf **Weiter**.
5. Tragen Sie die Telefonnummer ein, an die die Nachricht geschickt werden soll, und klicken Sie auf **Weiter**.
6. Tragen Sie den Geheimcode des vermissten Geräts ein und klicken Sie auf **Senden**.

PRIVATE DATEN VERBERGEN

Dieser Abschnitt informiert über die Komponente *Privatsphäre*. Diese Komponente kann sensible Benutzerdaten schützen, wenn das Gerät vorübergehend von einer anderen Person verwendet wird.

IN DIESEM ABSCHNITT

Über die Privatsphäre 83
Über die Modi der Privatsphäre 83
Privatsphären-Modus ändern 83
Privatsphäre automatisch starten 84
Privatsphäre ferngesteuert starten 85
Liste der geschützten Kontakte erstellen 87
Schutzobjekte wählen: Privatsphäre 89

ÜBER DIE PRIVATSPHÄRE

Die Komponente *Privatsphäre* schützt persönliche Daten und verhindert unbefugten Zugriff auf sensible Informationen, wenn Ihr Gerät vorübergehend von anderen Personen verwendet wird. Die Komponente kann vertrauliche Benutzerdaten verbergen. Dazu zählen Kontakte (die im Gerätespeicher, auf der SIM-Karte oder auf einem Wechseldatenträger gespeichert sind), Nachrichten und Anrufe.

Die Komponente *Privatsphäre* analysiert Daten auf Basis der Liste der geschützten Kontakte (s. Abschnitt "Schutzobjekte wählen: Privatsphäre" auf S. 89). Für Nummern aus dieser Liste verbirgt die Komponente folgende Informationen:

- Informationen in der Kontaktliste
- Einträge über eine Nummer in der Anrufliste (Angenommen, Gewählt, Unbeantwortet)
- SMS-Nachrichten in der Liste der eingehenden, ausgehenden, gelöschten und gesendeten SMS-Nachrichten

Informationen über die Arbeit der Privatsphäre werden in einem Bericht erfasst (s. Abschnitt "Programmberichte" auf S. 103).

ÜBER DIE MODI DER PRIVATSPHÄRE

Kaspersky Mobile Security 9.0 erlaubt es, den Schutz für persönliche Daten zu verwalten. Die Komponente *Privatsphäre* wird manuell gestartet. Sie ist standardmäßig deaktiviert.

Privatsphäre bietet folgende Modi:

- **Anzeigen** – Der Schutz für vertrauliche Daten ist deaktiviert. Die Einstellungen der Privatsphäre können geändert werden.
- **Verbergen** – Der Schutz für vertrauliche Daten ist aktiviert. Die Komponente *Privatsphäre* verbirgt alle Daten, die mit geschützten Kontakten zusammenhängen. Die Einstellungen der Privatsphäre können nicht geändert werden.

Der aktuelle Status der Komponente wird auf der Registerkarte **Privatsphäre** neben dem Menüpunkt **Modus** angezeigt.

Es kann eine gewisse Zeit beanspruchen, bis eine Modusänderung der Privatsphäre wirksam wird.

PRIVATSPHÄREN-MODUS ÄNDERN

Der Privatsphären-Modus kann folgendermaßen geändert werden:

- über die Programmoberfläche
- mit Hilfe des Geheimcodes, wenn sich das Gerät im aktiven Standby befindet

Gehen Sie folgendermaßen vor, um den Privatsphären-Modus zu ändern:

1. Wählen Sie auf der Registerkarte **Privatsphäre** den Punkt **Modus**.

   Das Fenster **Privatsphären-Modus** wird geöffnet.

2. Wählen Sie einen Wert für **Privatsphären-Modus** (s. Abb. unten).

Abbildung 47. Privatsphären-Modus ändern

3. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

➧ *Um den Privatsphären-Modus mit Hilfe des Geheimcodes zu ändern, wenn sich das Gerät im aktiven Standby-Modus befindet,*

geben Sie den ***Geheimcode#*** (z.B. *1234567#) ein.

Über den erfolgreich geänderten Privatsphären-Modus informiert eine Meldung.

PRIVATSPHÄRE AUTOMATISCH STARTEN

In der Grundeinstellung wird der Schutz für vertrauliche Daten sofort nach dem Einschalten der Privatsphäre gestartet.

Sie können eine Zeitspanne festlegen, nach deren Ablauf die Komponente *Privatsphäre* automatisch aktiviert werden soll.

Deaktivieren Sie die Privatsphäre, bevor die Einstellungen geändert werden sollen.

➧ *Gehen Sie folgendermaßen vor, um festzulegen, dass die Privatsphäre nach Ablauf eines bestimmten Zeitraums automatisch gestartet werden soll:*

1. Wählen Sie auf der Registerkarte **Privatsphäre** den Punkt **Modus**.

   Das Fenster **Privatsphären-Modus** wird geöffnet.

2. Legen Sie einen Zeitraum fest, nach dem die Komponente *Privatsphäre* automatisch gestartet werden soll. Wählen Sie dazu einen der folgenden Werte für **Automatisch verbergen** (s. Abb. unten):

   - **Sofort**
   - **In 1 Minute**
   - **In 5 Minuten**

- **In 15 Minuten**
- **In 1 Stunde**
- **Aus**

Abbildung 48. Einstellungen für den automatischen Start der Privatsphäre

3. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

PRIVATSPHÄRE FERNGESTEUERT STARTEN

Kaspersky Mobile Security 9.0 erlaubt es, die Privatsphäre mit einer speziellen SMS ferngesteuert zu starten. Dazu muss vorher die Funktion aktiviert werden, die den Remote-Start der Privatsphäre erlaubt.

➡ *Gehen Sie folgendermaßen vor, um den ferngesteuerten Start der Privatsphäre zu erlauben:*

1. Wählen Sie auf der Registerkarte **Privatsphäre** den Punkt **Modus**.

   Das Fenster **Privatsphären-Modus** wird geöffnet.

2. Wählen Sie für **Bei SMS verbergen** den Wert **Ja** (s. Abb. unten).

Abbildung 49. Einstellungen für das ferngesteuerte Aktivieren der Privatsphäre

3. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

Für den ferngesteuerten Start der Komponente *Privatsphäre* bestehen folgende Möglichkeiten:

- Befehl an das vermisste / gestohlene Gerät senden. Dafür ist ein anderes Gerät erforderlich, auf dem Kaspersky Mobile Security 9.0 installiert ist. Auf dem Zweitgerät wird mit Kaspersky Mobile Security 9.0 eine spezielle SMS-Nachricht erstellt und an das verlorene Gerät gesendet. Sie enthält die Telefonnummer des Geräts und seinen Geheimcode. Der Empfang einer speziellen SMS bleibt auf dem vermissten / gestohlenen Gerät unbemerkt.

- Mit den Standardfunktionen eines Handys, die zum Erstellen einer SMS-Nachricht dienen. Auf dem anderen Gerät wird eine SMS-Nachricht, die aus einem speziellen Text und dem Geheimcode des vermissten/gestohlenen Geräts besteht, erstellt und gesendet.

➧ *Gehen Sie folgendermaßen vor, um einen Befehl an das vermisste / gestohlene Gerät zu senden:*

1. Wählen Sie auf der Registerkarte **Erweitert** den Punkt **Befehl senden**.

   Ein Fenster zum Senden eines speziellen Befehls wird geöffnet.

2. Klicken Sie auf **Start**.

3. Wählen Sie den Befehlstyp **Privatsphäre** und klicken Sie auf **Weiter** (s. Abb. unten).

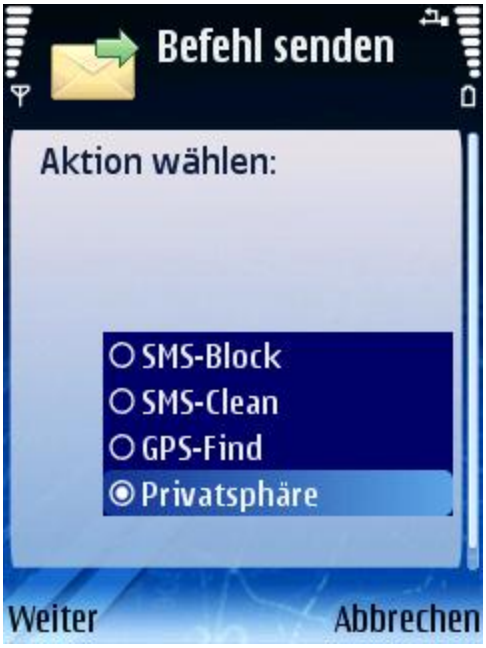


Abbildung 50. Privatsphäre ferngesteuert starten

4. Tragen Sie die Telefonnummer des Geräts ein, auf dem Daten verborgen werden sollen, und klicken Sie dann auf **Weiter**.

5. Tragen Sie den Geheimcode des vermissten Geräts ein und klicken Sie auf **Senden**.

Nach dem Empfang des Befehls wird die Komponente *Privatsphäre* automatisch auf dem verlorenen / gestohlenen Gerät gestartet.

➧ *Um mit Hilfe der Standardfunktionen eines Handys eine SMS zu erstellen:*

Schicken Sie an das Gerät eine SMS-Nachricht mit dem Text `hide:<Code>` (wobei `<Code>` der Geheimcode des vermissten Geräts ist). Die Groß- und Kleinschreibung von Buchstaben und die Leerzeichen vor und nach dem Doppelpunkt sind irrelevant.

LISTE DER GESCHÜTZTEN KONTAKTE ERSTELLEN

Die Komponente *Privatsphäre* verbirgt persönliche Daten (z.B. SMS-Nachrichten und Anrufe), die mit bestimmten Kontakten zusammenhängen. Solche Telefonnummern werden in der Liste der geschützten Kontakte gespeichert.

IN DIESEM ABSCHNITT

Nummer zur Liste der geschützten Kontakte hinzufügen 87

Nummer in der Liste der geschützten Kontakte ändern 88

Nummer aus der Liste der geschützten Kontakte löschen 89

NUMMER ZUR LISTE DER GESCHÜTZTEN KONTAKTE HINZUFÜGEN

Zur Liste der geschützten Kontakte können Sie beliebige Telefonnummern und Kontaktnamen hinzufügen, die auf der SIM-Karte oder im Telefonbuch des Geräts gespeichert sind.

Deaktivieren Sie die Privatsphäre, bevor die Einstellungen geändert werden sollen.

Gehen Sie folgendermaßen vor, um einen Eintrag zur Liste der geschützten Kontakte hinzuzufügen:

1. Wählen Sie auf der Registerkarte **Privatsphäre** den Punkt **Kontaktliste**.

   Das Fenster **Kontaktliste** wird geöffnet.

2. Führen Sie im nächsten Fenster eine der folgenden Aktionen aus (s. Abb. unten):

   - Um eine neue Nummer hinzuzufügen, gehen Sie auf **Optionen → Eintrag hinzufügen → Nummer**. Füllen Sie im folgenden Fenster **Nummer** das Feld **Nummer eingeben** aus. Klicken Sie zum Abschluss der Eingabe auf **OK**.

   - Um eine Nummer aus dem Telefonbuch hinzuzufügen, gehen Sie auf **Optionen → Eintrag hinzufügen → Kontakte**. Wählen Sie im folgenden Fenster **Kontakte** mit Hilfe des Menüs **Optionen → Auswählen** den entsprechenden Kontakt aus dem Telefonbuch. Klicken Sie zum Abschluss der Eingabe auf **OK**.

   - Um eine Nummer hinzuzufügen, die auf der SIM-Karte gespeichert ist, gehen Sie auf **Optionen → Eintrag hinzufügen → Kontakt von SIM**. Wählen Sie im folgenden Fenster **SIM-Kontakte** mit Hilfe des Menüs **Optionen → Auswählen** die entsprechende Nummer aus der Liste der SIM-Karte. Klicken Sie zum Abschluss der Eingabe auf **OK**.

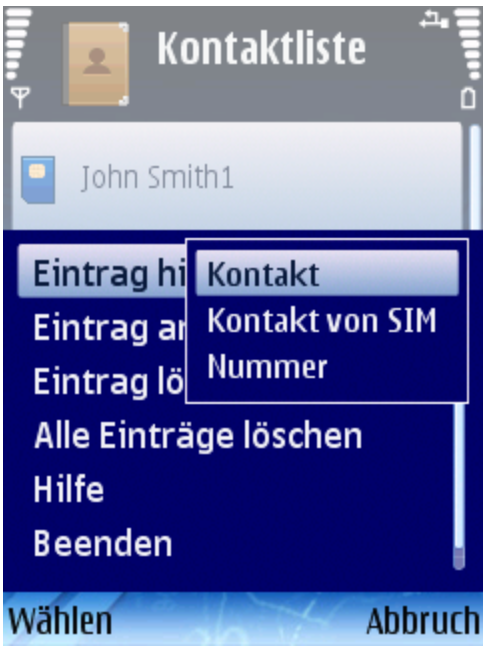


Abbildung 51. Nummer zur Liste der geschützten Kontakte hinzufügen

3. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

NUMMER IN DER LISTE DER GESCHÜTZTEN KONTAKTE ÄNDERN

Es können nur Nummern geändert werden, die direkt über das Programm eingegeben wurden. Nummern, die aus den Kontakten oder aus der SIM-Nummernliste übernommen wurden, können nicht geändert werden.

Deaktivieren Sie die Privatsphäre, bevor die Einstellungen geändert werden sollen.

Gehen Sie folgendermaßen vor, um eine Nummer in der Liste der geschützten Kontakte zu ändern:

1. Wählen Sie auf der Registerkarte **Privatsphäre** den Punkt **Kontaktliste**.

Das Fenster **Kontaktliste** wird geöffnet.

2. Markieren Sie in der Liste die Nummer, die Sie ändern möchten, und gehen Sie dann auf **Optionen → Eintrag ändern**.

   Auf dem Bildschirm erscheint die Telefonnummer des gewählten Kontakts.

3. Ändern Sie die Daten im Feld **Nummer eingeben**.

4. Klicken Sie zum Abschluss der Änderungen auf **OK**.

NUMMER AUS DER LISTE DER GESCHÜTZTEN KONTAKTE LÖSCHEN

Sie können eine Nummer löschen oder die gesamte Liste der geschützten Kontakte leeren.

- *Gehen Sie folgendermaßen vor, um eine Nummer zu löschen:*

1. Wählen Sie auf der Registerkarte **Privatsphäre** den Punkt **Kontaktliste**.

   Das Fenster **Kontaktliste** wird geöffnet.

2. Markieren Sie ein Element aus der Liste und gehen Sie dann auf **Optionen → Eintrag löschen**.

3. Bestätigen Sie das Löschen. Klicken Sie dazu auf **Ja**.

- *Gehen Sie folgendermaßen vor, um die Liste der geschützten Kontakte zu leeren:*

1. Wählen Sie auf der Registerkarte **Privatsphäre** den Punkt **Kontaktliste**.

   Das Fenster **Kontaktliste** wird geöffnet.

2. Gehen Sie auf **Optionen → Alle Einträge löschen**.

3. Bestätigen Sie das Löschen. Klicken Sie dazu auf **Ja**.

Die Liste der geschützten Kontakte wird geleert.

SCHUTZOBJEKTE WÄHLEN: PRIVATSPHÄRE

Wenn die Komponente *Privatsphäre* aktiviert ist, werden standardmäßig Kontakte, Nachrichten und Einträge in der Anrufliste verborgen, die mit geschützten Kontakten zusammenhängen. Sie können die Daten wählen, auf die der Zugriff verboten werden soll.

Deaktivieren Sie die Privatsphäre, bevor die Einstellungen geändert werden sollen.

- *Gehen Sie folgendermaßen vor, um die Schutzobjekte für geschützte Nummern zu wählen:*

1. Wählen Sie auf der Registerkarte **Privatsphäre** den Punkt **Verborgene Objekte**.

   Das Fenster **Verborgene Objekte** wird geöffnet.

2. Wählen Sie die Objekte, die für geschützte Nummern verborgen werden sollen. Legen Sie für die erforderlichen Parameter mit Hilfe des Menüs **Optionen → Ändern** den Wert **Verbergen** fest. Folgende Objekte können verborgen werden (s. Abb. unten):

   - **Kontakte** – Im Telefonbuch werden alle Daten über geschützte Nummern verborgen.

   - **Nachrichten** – In der Liste der eingehenden / ausgehenden SMS-Nachrichten werden alle SMS von geschützten Nummern verborgen.

- **Infos über Anrufe** – Anrufe von geschützten Nummern werden angenommen. Die Nummer des Anrufers wird aber ausgeblendet, und in der Anrufliste werden Infos über geschützte Nummern (Angenommen, Gewählt, Unbeantwortet) verborgen.

- **Eingehende Anrufe** – Anrufe von geschützten Nummern werden blockiert (Der Anrufer hört in diesem Fall ein "Besetzt"-Zeichen). Informationen über einen eingegangenen Anruf werden angezeigt, wenn die Komponente *Privatsphäre* deaktiviert wird.

- **Eingehende SMS** – Der Empfang eingehender SMS-Nachrichten wird nicht angezeigt (auf dem Display erscheint kein Hinweis darüber, dass eine neue SMS-Nachricht von einer verborgenen Nummer empfangen wurde). Alle SMS-Nachrichten, die von geschützten Nummern empfangen wurden, können gelesen werden, wenn die Komponente Privatsphäre deaktiviert wird.

Abbildung 52. Verborgene Objekte wählen

3. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

NETZWERKAKTIVITÄT FILTERN

Dieser Abschnitt informiert über die Komponente *Firewall,* die ein- und ausgehende Verbindungen auf Ihrem Gerät kontrolliert. Außerdem wird hier beschrieben, wie die Komponente aktiviert / deaktiviert wird und wie die gewünschte Sicherheitsstufe gewählt wird.

IN DIESEM ABSCHNITT

Firewall....91

Über die Sicherheitsstufen der Firewall....91

Sicherheitsstufe der Firewall wählen....91

Meldung über Verbindungsversuch....92

FIREWALL

Die Firewall analysiert alle Netzwerkverbindungen auf Ihrem Gerät. In Abhängigkeit der gewählten Sicherheitsstufe blockiert oder erlaubt sie bestimmte Netzwerkaktivitäten.

Die Firewall ist nach der Installation von Kaspersky Mobile Security 9.0 standardmäßig deaktiviert.

Um sich über alle blockierten Verbindungen informieren zu lassen, verwenden Sie die Firewall-Benachrichtigungen (s. Abschnitt "Meldung über Verbindungsversuch" auf S. 92).

Informationen über die Arbeit der Firewall werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. 103).

ÜBER DIE SICHERHEITSSTUFEN DER FIREWALL

Die Arbeit der Firewall ist von der ausgewählten Sicherheitsstufe abhängig. Die jeweils geltende Sicherheitsstufe definiert, über welche Netzwerkprotokolle die Datenübertragung zugelassen und über welche sie gesperrt wird.

Es sind folgende Sicherheitsstufen vorgesehen:

- **Aus** – jede Netzwerkaktivität erlauben. Diese Sicherheitsstufe ist standardmäßig aktiviert.
- **Nur eingehende Verbindungen verbieten** – nur eingehende Verbindungen blockieren. Ausgehende Verbindungen werden erlaubt.
- **Ausgehende SSH-, HTTP-, HTTPS-, IMAP-, SMTP-, POP3-Verbindungen erlauben** – alle eingehenden Verbindungen blockieren. Abholen / Senden von E-Mails, Anzeige von Webseiten und Download von Dateien sind erlaubt. Ausgehende Verbindungen können nur über die Ports SSH, HTTP, HTTPS, IMAP, SMTP, POP3 erfolgen.
- **Alle sperren** – jede Netzwerkaktivität außer Datenbank-Update und Lizenzverlängerung blockieren.

Sie können die Sicherheitsstufe der Firewall ändern (s. Abschnitt "Sicherheitsstufe der Firewall wählen" auf S. 91). Der aktuelle Modus wird auf der Registerkarte Firewall neben dem Menüpunkt **Modus** angezeigt.

SICHERHEITSSTUFE DER FIREWALL WÄHLEN

Um die Parameterwerte zu ändern, verwenden Sie den Joystick oder die Navigationstasten des Geräts oder gehen Sie auf **Optionen → Ändern**.

Gehen Sie folgendermaßen vor, um eine Sicherheitsstufe für die Firewall zu wählen:

1. Wählen Sie auf der Registerkarte **Firewall** den Punkt **Modus**.

   Das Fenster **Modus** wird geöffnet.

2. Wählen Sie eine Sicherheitsstufe (s. Abb. unten).

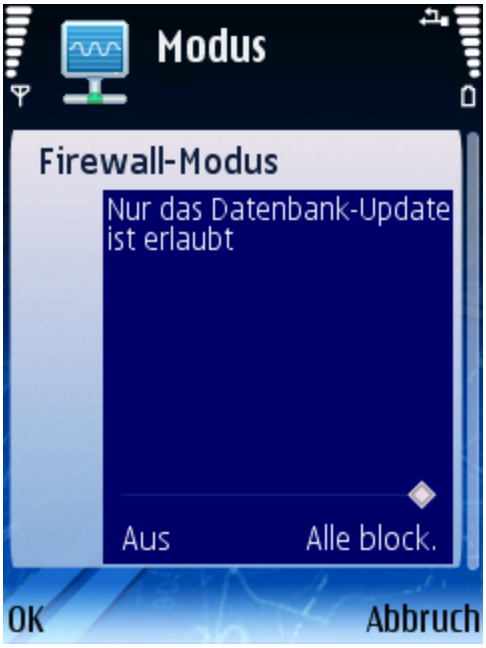


Abbildung 53. Sicherheitsstufe der Firewall wählen

3. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

MELDUNG ÜBER VERBINDUNGSVERSUCH

Die Firewall blockiert alle verbotenen Verbindungen entsprechend der gewählten Sicherheitsstufe (s. Abschnitt "Sicherheitsstufe der Firewall wählen" auf S. 91). Damit die Firewall Sie über alle blockierten Verbindungen auf dem mobilen Gerät informiert, verwenden Sie die Firewall-Benachrichtigungen.

- *Gehen Sie folgendermaßen vor, um Meldungen über einen Verbindungsversuch zu erhalten, der auf der aktuellen Firewall-Sicherheitsstufe verboten ist:*

1. Wählen Sie auf der Registerkarte **Firewall** den Punkt **Benachrichtigung**.

2. Setzen Sie den Parameter **Beim Blockieren** auf **Melden** (s. Abb. unten).

Abbildung 54. Firewall-Benachrichtigungen anpassen

3. Klicken Sie auf **OK**, um die Änderungen zu speichern.

PERSÖNLICHE DATEN VERSCHLÜSSELN

Dieser Abschnitt informiert über die Komponente *Verschlüsselung*, die sensible Daten auf Ihrem Gerät schützt. Außerdem wird hier beschrieben, wie die Komponente aktiviert / deaktiviert wird und wie ausgewählte Ordner verschlüsselt / entschlüsselt werden können.

IN DIESEM ABSCHNITT

Verschlüsselung 93

Daten verschlüsseln 94

Daten entschlüsseln 95

Zugriff auf verschlüsselte Daten verbieten 96

VERSCHLÜSSELUNG

Kaspersky Mobile Security 9.0 unterstützt die Datenverschlüsselung nicht auf mobilen Geräten mit dem Betriebssystem Symbian Series 60 5th Edition (9.4).

Die Komponente *Verschlüsselung* schützt die Daten auf dem Gerät auch dann vor dem Zugriff durch Dritte, wenn das Gerät in fremde Hände geraten sollte. Die Komponente erlaubt es, eine beliebige Anzahl von Ordnern, die nicht zum System gehören, zu verschlüsseln.

Um Daten zu entschlüsseln, muss der Geheimcode eingegeben werden. Wenn das Gerät in den Stromsparmodus gewechselt hat und die festgelegte Zeitspanne abgelaufen ist (s. Abschnitt "Zugriff auf verschlüsselte Daten verbieten" auf S. 96), wird der Datenzugriff automatisch blockiert.

Die Daten in einem Ordner werden durch den Befehl **Verschlüsseln** chiffriert. Künftig werden die Daten automatisch ver- und entschlüsselt, wenn Daten in dem Ordner gespeichert oder daraus gelesen werden oder wenn auf die Daten zugegriffen wird.

Die Komponente *Verschlüsselung* ist nach der Installation von Kaspersky Mobile Security 9.0 standardmäßig deaktiviert.

Informationen über die Arbeit der Komponente werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. 103).

DATEN VERSCHLÜSSELN

Die Komponente Verschlüsselung erlaubt es, eine beliebige Anzahl von Ordnern, die nicht zum System gehören, zu verschlüsseln. Die Ordner können sich im Speicher des Geräts oder auf einer Speicherkarte befinden.

Eine Liste aller bisher verschlüsselten und entschlüsselten Ordner befindet sich auf der Registerkarte **Verschlüsselung** unter dem Menüpunkt **Ordnerliste**.

Es ist auch möglich, alle Ordner, die in der Ordnerliste stehen, gleichzeitig zu verschlüsseln.

- *Gehen Sie folgendermaßen vor, um Daten zu verschlüsseln:*

1. Wählen Sie auf der Registerkarte **Verschlüsselung** den Punkt **Ordnerliste**.

   Das Fenster **Ordnerliste** wird geöffnet.

2. Gehen Sie auf **Optionen** → **Ordner hinzufügen** (s. Abb. unten).

Abbildung 55. Daten verschlüsseln

   Ein Fenster mit einer Übersicht des Dateisystems Ihres Geräts wird geöffnet.

3. Wählen Sie den Ordner, der verschlüsselt werden soll, und starten Sie dann die Verschlüsselung des Ordners. Gehen Sie dazu auf **Optionen** → **Verschlüsseln**.

   Um innerhalb des Dateisystems zu navigieren, verwenden Sie den Joystick oder die Navigationstasten des Geräts: **Nach oben** und **Nach unten** – zur Bewegung innerhalb des ausgewählten Ordners, **Nach links** und **Nach rechts** – zum Wechsel auf eine tiefere oder höhere Ebene des aktuellen Ordners.

4. Klicken Sie auf **OK**.

Der verschlüsselte Ordner wird zur Ordnerliste hinzugefügt.

Nach Abschluss des Verschlüsselungsvorgangs ändert sich im Menü **Optionen** der Punkt **Verschlüsseln** in **Entschlüsseln**.

Nach der Verschlüsselung werden Daten automatisch ent- und verschlüsselt, wenn Sie mit den Daten in einem verschlüsselten Ordner arbeiten, Daten aus einem verschlüsselten Ordner entnehmen oder neue Daten darin speichern.

- *Gehen Sie folgendermaßen vor, um alle Ordner der Liste auf einmal zu verschlüsseln:*

1. Wählen Sie auf der Registerkarte **Verschlüsselung** den Punkt **Ordnerliste**.

   Das Fenster **Ordnerliste** wird geöffnet.

2. Gehen Sie auf **Optionen** → **Zusatzaktionen** → **Alle verschlüsseln**.

3. Klicken Sie auf **OK**.

DATEN ENTSCHLÜSSELN

Sie können zuvor verschlüsselte Daten vollständig entschlüsseln (s. Abschnitt "Datenverschlüsselung" auf S. 94). Sie können einen oder alle verschlüsselten Ordner auf dem Gerät entschlüsseln.

- *Gehen Sie folgendermaßen vor, um einen zuvor verschlüsselten Ordner zu entschlüsseln:*

1. Wählen Sie auf der Registerkarte **Verschlüsselung** den Punkt **Ordnerliste**.

   Das Fenster **Ordnerliste** wird geöffnet. Es enthält eine Liste aller bisher ver- und entschlüsselten Ordner.

2. Wählen Sie in der Liste den Ordner, der entschlüsselt werden soll, und gehen Sie dann auf **Optionen** → **Entschlüsseln** (s. Abb. unten).

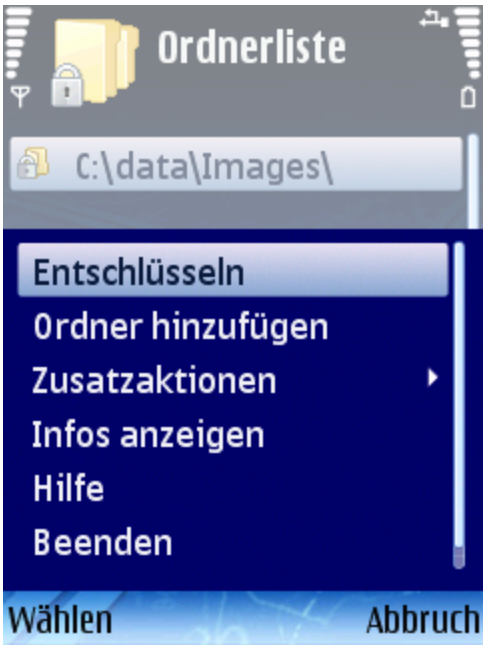


Abbildung 56. Daten entschlüsseln

3. Klicken Sie nach Abschluss der Entschlüsselung auf **OK**.

Nach Abschluss des Entschlüsselungsvorgangs ändert sich für den betreffenden Ordner im Menü **Optionen** der Punkt **Entschlüsseln** in **Verschlüsseln**. Sie können die Datenverschlüsselung erneut verwenden (s. Abschnitt "Daten verschlüsseln" auf S. 94).

Gehen Sie folgendermaßen vor, um alle Ordner der Liste auf einmal zu entschlüsseln:

1. Wählen Sie auf der Registerkarte **Verschlüsselung** den Punkt **Ordnerliste**.

   Das Fenster **Ordnerliste** wird geöffnet.

2. Gehen Sie auf **Optionen** → **Zusatzaktionen** → **Alle entschlüsseln**.

3. Klicken Sie auf **OK**.

ZUGRIFF AUF VERSCHLÜSSELTE DATEN VERBIETEN

Die Komponente *Verschlüsselung* kann den Zugriff auf verschlüsselte Daten entweder sofort blockieren oder nach Ablauf einer festgelegten Zeitspanne ab dem Wechsel des Geräts in den Stromsparmodus.

Standardmäßig wird der Zugriff auf verschlüsselte Daten sofort blockiert, nachdem sich die Hintergrundbeleuchtung des Bildschirms ausschaltet.

Sie können festlegen, nach welchem Zeitraum verschlüsselte Daten blockiert werden sollen, wenn das Gerät in den Stromsparmodus wechselt. Um künftig mit verschlüsselten Daten zu arbeiten, muss der Geheimcode eingegeben werden.

Außerdem können Sie den Zugriff auf verschlüsselte Daten sofort verbieten und die Abfrage des Geheimcodes aktivieren.

Gehen Sie folgendermaßen vor, um den Zugriff auf einen Zugriff zeitverzögert zu verbieten:

1. Wählen Sie auf der Registerkarte **Verschlüsselung** den Punkt **Zugriff verbieten**.

   Das Fenster **Zugriff verbieten** wird geöffnet.

2. Legen Sie fest, wie lange die Daten noch verfügbar sein sollen, nachdem das Gerät in den Stromsparmodus gewechselt hat. Wählen Sie dazu einen der folgenden Werte (s. Abb. unten):

   - **Sofort**
   - **In 1 Minute**
   - **In 5 Minuten**
   - **In 15 Minuten**

- **In 1 Stunde**

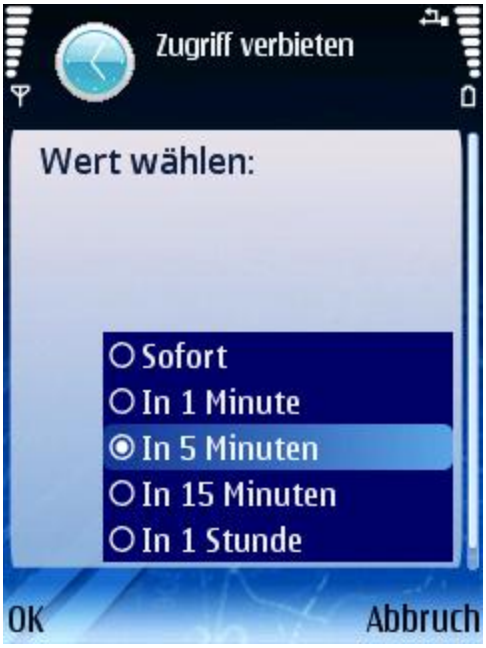


Abbildung 57. Zugriff auf verschlüsselte Daten blockieren

3. Klicken Sie auf **OK**, um die Änderungen zu speichern.

➡ *Um den Zugriff auf verschlüsselte Daten sofort zu verbieten und die Abfrage des Geheimcodes zu aktivieren,*

drücken Sie auf dem Gerät gleichzeitig "0" und "1".

UPDATE DER PROGRAMM-DATENBANKEN

Dieser Abschnitt informiert über das Update der Programm-Datenbanken. Das Update hält den Schutz Ihres Geräts auf dem neusten Stand. Außerdem werden hier folgende Vorgänge beschrieben: Informationen über die installierten Programm-Datenbanken anzeigen, Updatevorgang manuell starten, automatisches Datenbank-Update anpassen.

IN DIESEM ABSCHNITT

Über das Update der Programm-Datenbanken....98

Datenbankinfos anzeigen....98

Update manuell starten....99

Update nach Zeitplan starten....100

Update im Roaming....101

Einstellungen der Internetverbindung anpassen....102

ÜBER DAS UPDATE DER PROGRAMM-DATENBANKEN

Die Suche erfolgt auf Basis von Programm-Datenbanken, die eine Beschreibung aller momentan bekannten schädlichen Programme und entsprechende Desinfektionsmethoden sowie eine Beschreibung sonstiger unerwünschter Objekte enthalten. Es ist sehr wichtig, die Datenbanken auf dem neuesten Stand zu halten.

Es wird empfohlen, die Programm-Datenbanken regelmäßig zu aktualisieren. Die Daten gelten als stark veraltet, wenn seit dem letzten Update 15 Tage vergangen sind. In diesem Fall kann die Zuverlässigkeit des Schutzes nicht mehr garantiert werden.

Kaspersky Mobile Security 9.0 lädt seine Updates von Kaspersky-Lab-Updateservern herunter. Dabei handelt es sich um spezielle Internetseiten, auf denen Updates der Datenbanken für alle Kaspersky-Lab-Produkte zur Verfügung gestellt werden.

Um die Programm-Datenbanken zu aktualisieren, muss auf dem mobilen Gerät eine Internetverbindung eingerichtet sein.

Die Aktualisierung der Programm-Datenbanken wird nach folgendem Ablauf ausgeführt:

1. Die Programm-Datenbanken auf Ihrem mobilen Gerät werden mit den Datenbanken verglichen, die sich auf dem Kaspersky-Lab-Updateserver befinden.

2. Kaspersky Mobile Security 9.0 führt eine der folgenden Aktionen aus:

   - Wenn Ihre Programm-Datenbanken aktuell sind, wird eine entsprechende Meldung angezeigt.

   - Wenn sich die installierten Datenbanken von den angebotenen unterscheiden, wird ein neues Updatepaket heruntergeladen und installiert.

     Die Verbindung wird nach Abschluss des Updatevorgangs automatisch getrennt. Eine Verbindung, die bereits vor dem Update aufgebaut wurde, bleibt bestehen.

In der Grundeinstellung werden die Einstellungen der Internetverbindung automatisch ermittelt. Falls die Verbindungseinstellungen nicht automatisch ermittelt werden, passen Sie die Verbindung an (s. Abschnitt "Einstellungen für Internetverbindung anpassen" auf S. 102).

Sie können die Updateaufgabe entweder manuell starten, wenn das Gerät nicht für andere Aufgaben benötigt wird, oder einen Zeitplan für das automatische Update einstellen.

Wenn sich ein Gerät im Roaming befindet, kann das Update der Datenbanken für Kaspersky Mobile Security 9.0 deaktiviert werden, um erhöhte Kosten zu vermeiden.

Das Erscheinungsdatum der Datenbanken wird im Fenster für den Schutzstatus genannt (s. Abschnitt "Fenster für den Schutzstatus" auf S. 34). Detaillierte Angaben über die verwendeten Datenbanken befinden sich auf der Registerkarte **Erweitert** im Menüpunkt **Datenbankinfos**.

Informationen über das Datenbank-Update werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. 103).

DATENBANKINFOS ANZEIGEN

Sie können Informationen über die installierten Programm-Datenbanken anzeigen. Folgende Daten sind verfügbar: Datum des letzten Updates, Erscheinungsdatum der Datenbanken und Anzahl der Einträge in den Datenbanken.

- *Um Informationen über die installierten Datenbanken anzuzeigen,*

  auf der Registerkarte **Erweitert** den Punkt **Datenbank-Infos** (s. Abb. unten).

Abbildung 58. Informationen über die installierten Programm-Datenbanken

UPDATE MANUELL STARTEN

Sie können das Update der Programm-Datenbanken manuell starten.

- *Gehen Sie folgendermaßen vor, um das Update der Programm-Datenbanken manuell zu starten:*

  1. Wählen Sie auf der Registerkarte **Anti-Virus** den Punkt **Update**.

     Das Fenster **Update** wird geöffnet.

2. Gehen Sie auf **Update** (s. Abb. unten).

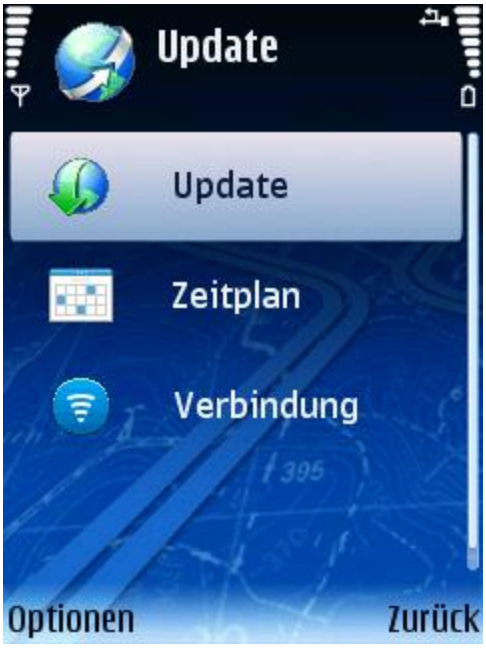


Abbildung 59. Update manuell starten

Das Programm startet das Update der Datenbanken von einem Kaspersky-Lab-Server. Informationen über den Updatevorgang werden auf dem Bildschirm angezeigt.

UPDATE NACH ZEITPLAN STARTEN

Eine wichtige Voraussetzung für die Sicherheit des Geräts besteht darin, den Schutz auf dem neusten Stand zu halten. Sie können das automatische Update der Datenbanken festlegen.

Zusätzlich können Sie das automatische Update für den Fall anpassen, dass Sie sich im Roaming befinden (s. Abschnitt "Update im Roaming" auf S. 101).

➡ *Um einen Zeitplan einzurichten, nach dem die Datenbanken automatisch aktualisiert werden:*

1. Wählen Sie auf der Registerkarte **Anti-Virus** den Punkt **Update**.

   Das Fenster **Update** wird geöffnet.

2. Gehen Sie auf **Zeitplan**.

   Das Fenster **Zeitplan** wird geöffnet.

3. Wählen Sie einen der folgenden Werte für **Auto-Update** (s. Abb. unten):

   - **Aus**: Die Programm-Datenbanken werden nicht nach Zeitplan aktualisiert.
   - **Wöchentlich**: Die Programm-Datenbanken werden ein Mal in der Woche aktualisiert. Legen Sie zusätzlich **Update-Tag** und **Update-Zeit** fest.

- **Täglich**: Die Programm-Datenbanken werden jeden Tag aktualisiert. Legen Sie dafür eine **Update-Zeit** fest.

Abbildung 60. Einstellungen für automatisches Update

4. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

UPDATE IM ROAMING

Sie können festlegen, dass das geplante Update der Programm-Datenbanken im Roaming deaktiviert wird. Das manuelle Update steht weiterhin zur Verfügung.

Gehen Sie folgendermaßen vor, um das geplante Update im Roaming zu deaktivieren:

1. Wählen Sie auf der Registerkarte **Anti-Virus** den Punkt **Update**.

   Das Fenster **Update** wird geöffnet.

2. Gehen Sie auf **Zeitplan**.

   Das Fenster **Zeitplan** wird geöffnet.

3. Setzen Sie **Im Roaming erlauben** auf **Nein** (s. Abb. unten).

Abbildung 61. Update im Roaming anpassen

4. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

EINSTELLUNGEN DER INTERNETVERBINDUNG ANPASSEN

Kaspersky Mobile Security 9.0 verwendet den standardmäßig festgelegten Access Point für die Internetverbindung.

Die Parameter für den Access Point stellt der Dienstanbieter zur Verfügung.

Falls Kaspersky Mobile Security 9.0 die Verbindungseinstellungen nicht automatisch ermittelt, passen Sie die Einstellungen an.

Gehen Sie folgendermaßen vor, um die Einstellungen der Internetverbindung anzupassen:

1. Wählen Sie auf der Registerkarte **Anti-Virus** den Punkt **Update**.

   Das Fenster **Update** wird geöffnet.

2. Gehen Sie auf **Verbindung**.

3. Markieren Sie den Access Point, der für die Verbindung zum Updateserver dient. Wählen Sie dazu einen Wert für **Access Point** und klicken Sie dann auf **OK** (s. Abb. unten).

Die Liste zeigt alle Access Points, die auf dem mobilen Gerät eingerichtet sind.

Abbildung 62. Einstellungen der Internetverbindung

4. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

PROGRAMMBERICHTE

Dieser Abschnitt informiert über die Berichte, in denen die Arbeit der einzelnen Komponenten und die Ausführung aller Aufgaben (z.B. Update der Programm-Datenbanken, Virensuche, usw.) protokolliert werden.

IN DIESEM ABSCHNITT

Berichte 103

Berichtseinträge anzeigen 103

Berichtseinträge löschen 104

BERICHTE

In Berichten werden Ereignisse gespeichert, die bei der Arbeit der einzelnen Komponenten von Kaspersky Mobile Security 9.0 auftreten. Die Einträge sind in absteigender Reihenfolge nach dem Zeitpunkt der Ereignisse angeordnet.

Für jede Komponente wird ein eigener Ereignisbericht geführt.

BERICHTSEINTRÄGE ANZEIGEN

➧ *Gehen Sie folgendermaßen vor, um die Einträge im Bericht einer Komponente anzuzeigen:*

1. Wählen Sie auf der Registerkarte der entsprechenden Komponente den Punkt **Bericht**.

Der Bericht der gewählten Komponente wird geöffnet (s. Abb. unten).

Abbildung 63. Bericht für eine bestimmte Komponente

2. Verwenden Sie zur Navigation in einem Bericht den Joystick oder die Navigationstasten : **Aufwärts** und **Abwärts** – Ereignisse im aktuellen Bericht anzeigen, **Nach links** und **Nach rechts** – zu Berichten für andere Komponenten wechseln.

- *Um ausführliche Informationen über einen Berichtseintrag anzuzeigen,*

  wählen Sie einen Eintrag und gehen Sie dann auf **Optionen → Infos anzeigen**.

BERICHTSEINTRÄGE LÖSCHEN

Sie können alle Berichte leeren. Die Informationen über die Arbeit aller Komponenten von Kaspersky Mobile Security 9.0 werden gelöscht.

- *Gehen Sie folgendermaßen vor, um alle Einträge aus einem Bericht zu löschen:*

  1. Wählen Sie auf der Registerkarte einer beliebigen Komponente den Punkt **Bericht**.

     Das Fenster **Bericht** wird geöffnet.

  2. Gehen Sie auf **Optionen → Bericht leeren**.

Es werden alle Einträge im Bericht aller Komponenten gelöscht.

ERWEITERTE EINSTELLUNGEN ANPASSEN

Dieser Abschnitt informiert über zusätzliche Optionen von Kaspersky Mobile Security 9.0: Geheimcode ändern, Audiosignale des Programms und Hintergrundbeleuchtung des Bildschirms verwalten, Anzeige des Schutzsymbols und des Statusfensters aktivieren / deaktivieren.

IN DIESEM ABSCHNITT

Geheimcode ändern 105

Tooltips anzeigen 105

Audiosignale verwalten 105

Hintergrundbeleuchtung verwalten 106

Statusfenster anzeigen 107

Schutzsymbol anzeigen 108

GEHEIMCODE ÄNDERN

Der Geheimcode, der nach der Programmaktivierung festgelegt wurde, kann geändert werden.

Gehen Sie folgendermaßen vor, um den Geheimcode zu ändern:

1. Wählen Sie auf der Registerkarte **Erweitert** den Punkt **Einstellungen**.

   Das Fenster **Einstellungen** wird geöffnet.

2. Gehen Sie auf **Code ändern**.

3. Geben Sie im Feld **Code eingeben** den aktuellen Code ein und klicken Sie auf **OK**.

4. Geben Sie im Feld **Neuen Code eingeben** einen neuen Code ein und klicken Sie auf **OK**, um die Änderungen zu speichern.

TOOLTIPS ANZEIGEN

Während Sie die Einstellungen der Komponenten anpassen, zeigt Kaspersky Mobile Security 9.0 standardmäßig kurze Tooltips für die jeweilige Funktion an. Die Anzeige von Tooltips für Kaspersky Mobile Security 9.0 lässt sich anpassen.

Gehen Sie folgendermaßen vor, um die Anzeige von Tooltips anzupassen:

1. Wählen Sie auf der Registerkarte **Erweitert** den Punkt **Einstellungen**.

   Das Fenster **Einstellungen** wird geöffnet.

2. Wählen Sie einen Wert für **Tooltips**:

   - **Anzeigen** – Tooltips anzeigen, bevor eine Funktion angepasst wird
   - **Verbergen** – keine Tooltips anzeigen

3. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

AUDIOSIGNALE VERWALTEN

Bei der Arbeit des Programms treten unterschiedliche Ereignisse auf. Dazu zählen beispielsweise der Fund eines infizierten Objekts oder eines Virus, der Ablauf der Lizenz usw. Damit das Programm Sie über solche Ereignisse informiert, können Sie entsprechende Audiosignale aktivieren.

In der Grundeinstellung aktiviert Kaspersky Mobile Security 9.0 die Audiosignale nur entsprechend dem für das Gerät festgelegten Modus.

Um die Parameterwerte zu ändern, verwenden Sie den Joystick oder die Navigationstasten des Geräts oder gehen Sie auf **Optionen → Ändern**.

Gehen Sie folgendermaßen vor, um die Audiosignale des Programms zu verwalten:

1. Wählen Sie auf der Registerkarte **Erweitert** den Punkt **Einstellungen**.

   Das Fenster **Einstellungen** wird geöffnet.

2. Wählen Sie einen Wert für **Audiosignale** (s. Abb. unten):

   - **Immer** – unabhängig vom aktuellen Geräteprofil immer Audiosignale verwenden
   - **Nach Modus** – Audiosignale in Abhängigkeit des gewählten Gerätemodus verwenden
   - **Deaktivieren** – keine Audiosignale verwenden

Abbildung 64. Audiosignale verwalten

3. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

HINTERGRUNDBELEUCHTUNG VERWALTEN

Wenn das Programm Schutzaufgaben ausführt, wird auf dem Gerät zusätzlich Strom verbraucht. Um während der Aufgabenausführung Strom zu sparen, kann das Programm die Hintergrundbeleuchtung automatisch ausschalten.

Um die Parameterwerte zu ändern, verwenden Sie den Joystick oder die Navigationstasten des Geräts oder gehen Sie auf **Optionen → Ändern**.

Gehen Sie folgendermaßen vor, damit die Hintergrundbeleuchtung während der Aufgabenausführung ausgeschaltet wird:

1. Wählen Sie auf der Registerkarte **Erweitert** den Punkt **Einstellungen**.

Das Fenster **Einstellungen** wird geöffnet.

2. Wählen Sie einen Wert für **Hintergrundbeleuchtung** (s. Abb. unten):

   - **Nach Modus** – Hintergrundbeleuchtung in Abhängigkeit des gewählten Gerätemodus verwenden
   - **Aktivieren** – Hintergrundbeleuchtung immer verwenden

Abbildung 65. Hintergrundbeleuchtung verwalten

3. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

STATUSFENSTER ANZEIGEN

Sie können einstellen, dass ob das Statusfenster bei Programmstart angezeigt wird oder nicht.

Um die Parameterwerte zu ändern, verwenden Sie den Joystick oder die Navigationstasten des Geräts oder gehen Sie auf **Optionen → Ändern**.

Gehen Sie folgendermaßen vor, um festzulegen, ob das Statusfenster bei Programmstart angezeigt wird:

1. Wählen Sie auf der Registerkarte **Erweitert** den Punkt **Einstellungen**.

   Das Fenster **Einstellungen** wird geöffnet.

2. Wählen Sie einen Wert für **Statusfenster** (s. Abb. unten):

   - **Anzeigen** – Statusfenster anzeigen

- **Verbergen** – Statusfenster nicht anzeigen

Abbildung 66. Anzeige des Statusfensters anpassen

3. Klicken Sie auf **Zurück**, um die Änderungen zu speichern.

SCHUTZSYMBOL ANZEIGEN

Sie können die Anzeige des Statussymbols auf dem Display des mobilen Geräts so anpassen, dass der Schutzstatus sichtbar ist (s. Abschnitt "Schutzsymbol" auf S. 34).

Um die Parameterwerte zu ändern, verwenden Sie den Joystick oder die Navigationstasten des Geräts oder gehen Sie auf **Optionen → Ändern**.

Gehen Sie folgendermaßen vor, um die Anzeige des Schutzsymbols anzupassen:

1. Wählen Sie auf der Registerkarte **Anti-Virus** den Punkt **Schutz**.

   Das Fenster **Schutz** wird geöffnet.

2. Wählen Sie einen Wert für den Parameter **Schutzsymbol** (s. Abb. unten):

   - **Immer anzeigen** – Schutzsymbol auf dem Gerätedisplay anzeigen
   - **Nur im Menü** – Schutzsymbol nur anzeigen, wenn das Gerätemenü oder das Menü von Kaspersky Mobile Security 9.0 geöffnet ist

- **Nicht anzeigen** – Schutzsymbol nicht anzeigen

Abbildung 67. Einstellungen für die Anzeige des Schutzsymbols

3. Klicken Sie auf **OK**, um die Änderungen zu speichern.

KASPERSKY MOBILE SECURITY 9.0 FÜR MICROSOFT WINDOWS MOBILE

In diesem Kapitel wird die Funktionsweise von Kaspersky Mobile Security 9.0 für mobile Geräte beschrieben, die mit einem der folgenden Betriebssysteme arbeiten:

- Microsoft Windows Mobile 5.0
- Microsoft Windows Mobile 6.0, 6.1, 6.5

IN DIESEM ABSCHNITT

Kaspersky Mobile Security 9.0 installieren....110

Programm deinstallieren....111

Upgrade von Programmversion 8.0 auf Version 9.0....113

Erste Schritte....114

Programmoberfläche....124

Schutz für das Dateisystem....127

Untersuchung des Geräts....130

Quarantäne für schädliche Objekte....137

Eingehende Anrufe und SMS-Nachrichten filtern....139

Ausgehende Anrufe und SMS-Nachrichten einschränken. Kindersicherung....152

Datenschutz bei Verlust oder Diebstahl des Geräts....160

Persönliche Daten verbergen....171

Netzwerkaktivität filtern. Firewall....180

Persönliche Daten verschlüsseln....181

Update der Programm-Datenbanken....186

Programmberichte....191

Erweiterte Einstellungen anpassen....193

KASPERSKY MOBILE SECURITY 9.0 INSTALLIEREN

Die Installation des Programms auf einem mobilen Gerät umfasst mehrere Schritte.

Es wird empfohlen, vor Beginn der Installation alle anderen Programme auf dem mobilen Gerät zu schließen.

Gehen Sie folgendermaßen vor, um Kaspersky Mobile Security zu installieren:

1. Verwenden Sie für die Verbindung des mobilen Geräts mit dem Computer das Programm Microsoft ActiveSync.
2. Führen Sie eine der folgende Aktionen aus:
   - Wenn Sie das Programm auf CD erworben haben, starten Sie auf der CD die automatische Installation von Kaspersky Mobile Security 9.0.
   - Wenn Sie die Installationsdatei über das Internet bezogen haben, kopieren Sie sie auf das mobile Gerät. Dazu stehen folgende Methoden zur Verfügung:
     - von der Webseite von Kaspersky Lab
     - mit dem Programm Microsoft ActiveSync
     - mit einer Speicherkarte

     Starten Sie anschließend die Installation (öffnen Sie das CAB-Archiv auf dem mobilen Gerät).
3. Lesen Sie den Lizenzvertrag, der zwischen Ihnen und Kaspersky Lab abgeschlossen wird. Klicken Sie auf **OK**, wenn Sie die Vertragsbedingungen akzeptieren. Danach wird Kaspersky Mobile Security 9.0 auf dem Gerät installiert. Klicken Sie auf **Abbrechen**, wenn Sie den Bedingungen des Lizenzvertrags nicht zustimmen.
4. Wählen Sie eine Sprache für die Oberfläche von Kaspersky Mobile Security 9.0 und klicken Sie auf **OK**.
5. Starten Sie das Gerät neu, um die Installation abzuschließen. Klicken Sie dazu auf **Neustart**.

   Das Programm wird mit den von Kaspersky Lab empfohlenen Einstellungen installiert.

PROGRAMM DEINSTALLIEREN

Gehen Sie folgendermaßen vor, um Kaspersky Mobile Security 9.0 zu löschen.

1. Entschlüsseln Sie die Daten auf Ihrem Gerät, wenn diese mit Kaspersky Mobile Security verschlüsselt wurden (s. Abschnitt "Daten entschlüsseln" auf S. 183).
2. Deaktivieren Sie die Privatsphäre (s. Abschnitt "Privatsphäre aktivieren / deaktivieren" auf S. 172).
3. Beenden Sie Kaspersky Mobile Security 9.0. Gehen Sie dazu auf **Menü → Beenden**.
4. Entfernen Sie Kaspersky Mobile Security 9.0. Gehen Sie dazu folgendermaßen vor:
   a. Klicken Sie auf **Start → Einstellungen**.

b. Wählen Sie auf der Registerkarte **System** den Punkt **Programme entfernen** (s. Abb. unten).

*Abbildung 68. Registerkarte **System***

c. Wählen Sie in der Liste der installierten Programme **Kaspersky Mobile Security** und klicken Sie auf **Entfernen** (s. Abb. unten).

Abbildung 69. Zu löschendes Programm wählen

d. Bestätigen Sie die Deinstallation im folgenden Fenster mit **Ja**.

e. Geben Sie den Geheimcode ein und klicken Sie auf **OK**.

f. Legen Sie fest, ob Programmeinstellungen und Quarantäneobjekte gespeichert werden sollen: (s. Abb. unten):

- Wenn Sie die Programmeinstellungen und Quarantäneobjekte speichern möchten, klicken Sie auf **Speichern**.
- Klicken Sie auf **Löschen**, um das Programm vollständig zu deinstallieren.

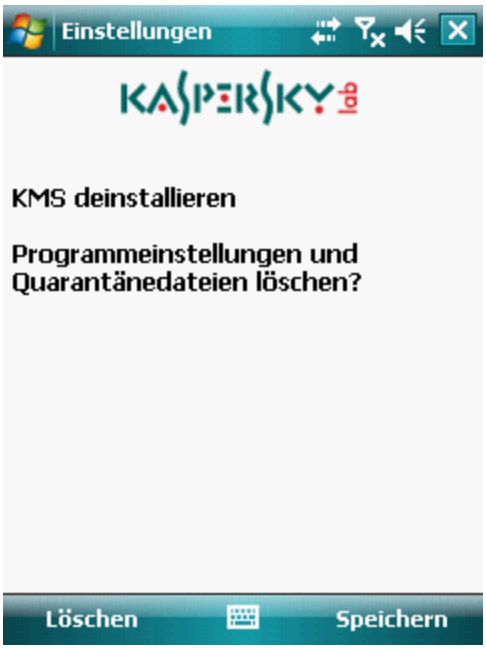


Abbildung 70. Programmeinstellungen löschen

5. Starten Sie das Gerät neu, um die Deinstallation des Programms abzuschließen.

UPGRADE VON PROGRAMMVERSION 8.0 AUF VERSION 9.0

Wenn auf Ihrem Gerät bereits Kaspersky Mobile Security 8.0 installiert ist, können Sie es auf Kaspersky Mobile Security 9.0 aktualisieren.

Bevor Sie das Programm auf eine andere Version upgraden, deaktivieren Sie die Verschlüsselung und entschlüsseln Sie alle Daten (s. Abschnitt "Daten entschlüsseln" auf S. 183).

➡ *Gehen Sie folgendermaßen vor, um das Programm auf die neue Version zu aktualisieren:*

1. Beenden Sie die aktuelle Version von Kaspersky Mobile Security. Gehen Sie dazu auf **Menü → Beenden**.
2. Kopieren Sie die Distribution auf das Gerät. Dazu stehen folgende Methoden zur Verfügung:
   - von der Webseite von Kaspersky Lab
   - mit dem Programm Microsoft ActiveSync
   - mit einer Speicherkarte
3. Starten Sie auf dem Gerät das Setup für Kaspersky Mobile Security 9.0.
4. Lesen Sie den Lizenzvertrag genau. Wenn Sie den Vertragsbestimmungen zustimmen, klicken Sie auf **Akzeptieren**. Ihnen wird vorgeschlagen, zuerst die installierte Version 8.0 zu entfernen.

5. Bestätigen Sie die Deinstallation von Programmversion 8.0 mit **OK**.

6. Geben Sie den Geheimcode aus der Vorgängerversion des Programms ein.

7. Löschen Sie die Einstellungen, die in der vorherigen Programmversion verwendet wurden. Klicken Sie dazu auf **Löschen**.

   Die Einstellungen können nur gespeichert werden, wenn ein Wechsel zwischen Versionen der gleichen Produktgeneration erfolgt. Die Programmeinstellungen von 8.0 sind nicht mit Programmversion 9.0 kompatibel.

8. Starten Sie das Gerät neu, um den Deinstallationsvorgang abzuschließen. Klicken Sie dazu auf **Neustart**.

9. Starten Sie nach dem Neustart des Geräts die Installation von Kaspersky Mobile Security 9.0 (s. Abschnitt "Kaspersky Mobile Security 9.0 installieren" auf S. 110).

   Wenn die Lizenz für Kaspersky Mobile Security 8.0 noch gültig ist, aktivieren Sie die Programmversion 9.0 mit dem Aktivierungscode von Version 8.0 (s. Abschnitt "Programm aktivieren" auf S. 114).

ERSTE SCHRITTE

Dieser Abschnitt informiert darüber, wie Kaspersky Mobile Security 9.0 für den Einsatz vorbereitet wird (Programm aktivieren und Geheimcode festlegen), das Programm gestartet und das Gerät auf Viren untersucht wird.

IN DIESEM ABSCHNITT

Programm aktivieren....114

Geheimcode eingeben....117

Programm starten....118

Update der Programm-Datenbanken....118

Gerät auf Viren untersuchen....118

Programm-Info anzeigen....119

Lizenzverwaltung....119

PROGRAMM AKTIVIEREN

Um mit Kaspersky Mobile Security 9.0 zu arbeiten, muss das Programm aktiviert werden. Bei der Programmaktivierung wird der Aktivierungscode eingegeben, der dann auf den Kaspersky-Lab-Servern geprüft und registriert wird. Anschließend lädt das Programm eine Schlüsseldatei herunter und installiert diese.

Ein Aktivierungscode kann folgendermaßen erworben werden:

- online (s. Abschnitt "Aktivierungscode online kaufen" auf S. 117). Dazu wird direkt aus Kaspersky Mobile Security 9.0 die Website http://www.kaspersky.com/gotopartnersite/def72/buy aufgerufen.
- auf der Webseite http://www.kaspersky.de/store
- im Fachhandel

Um Kaspersky Mobile Security auf einem Gerät zu aktivieren, ist eine Internetverbindung erforderlich.

Stellen Sie vor der Programmaktivierung sicher, dass Datum und Uhrzeit des Gerätesystems korrekt eingestellt sind.

Das Programm kann auf folgende Weise aktiviert werden:

- **Testversion aktivieren**. Wählen Sie diese Aktivierungsmethode, wenn Sie das Programm zuerst testen und später eine kommerzielle Programmversion kaufen möchten. Bei der Aktivierung wird eine kostenlose Schlüsseldatei installiert. Die Gültigkeit der Testlizenz wird nach der Aktivierung auf dem Bildschirm angezeigt. Nach Ablauf der Testlizenz werden die Programmfunktionen eingeschränkt. Es stehen nur noch folgende Einstellungen zur Verfügung:

  - Programm aktivieren
  - Programmlizenzen verwalten
  - Hilfesystem für Kaspersky Mobile Security 9.0
  - Verschlüsselung deaktivieren
  - Privatsphäre deaktivieren

  Es ist nicht möglich, eine weitere Testlizenz zu aktivieren.

- **Kommerzielle Version aktivieren**. Wählen Sie diese Variante, wenn Sie eine kommerzielle Programmversion erworben und einen Aktivierungscode erhalten haben. Nach Eingabe des Aktivierungscodes wird eine Schlüsseldatei empfangen und installiert. Nun können Sie das Programm im vollen Funktionsumfang nutzen. Die Gültigkeit der Lizenz wird auf dem Bildschirm angezeigt. Nach Ablauf der Gültigkeit wird die Programmfunktionalität eingeschränkt. Es wird keine Programmaktualisierung mehr ausgeführt.

IN DIESEM ABSCHNITT

Kommerzielle Version aktivieren.....115

Testversion aktivieren.....116

Aktivierungscode online kaufen.....117

KOMMERZIELLE VERSION AKTIVIEREN

Gehen Sie folgendermaßen vor, um eine kommerzielle Programmversion mit einem Aktivierungscode zu aktivieren:

1. Gehen Sie auf **Start** → **Programme**.
2. Wählen Sie **KMS 9.0** und starten Sie das Programm. Verwenden Sie dazu den Stylus oder die mittlere Joystick-Taste.

   Das Fenster **Aktivierung** wird geöffnet.
3. Gehen Sie auf **Code eingeben**.

   Das Aktivierungsfenster für Kaspersky Mobile Security 9.0 wird geöffnet (s. Abb. unten).

4. Geben Sie den Code in die entsprechenden vier Felder ein und klicken Sie dann auf **Weiter**.

Abbildung 71. Kommerzielle Version aktivieren

5. Bestätigen Sie die Internetverbindung mit **Ja**.

   Das Programm sendet eine Anfrage an den Aktivierungsserver von Kaspersky Lab, lädt eine Schlüsseldatei herunter und installiert sie.

   Wenn der von Ihnen eingegebene Aktivierungscode ungültig ist, erscheint eine entsprechende Meldung auf dem Bildschirm des mobilen Geräts. Prüfen Sie in diesem Fall, ob der Aktivierungscode richtig eingegeben wurde, und wenden Sie sich dann an die Firma, bei der Sie den Aktivierungscode für Kaspersky Mobile Security 9.0 gekauft haben.

   Wenn bei der Verbindung mit dem Server Fehler aufgetreten sind und der Download einer Schlüsseldatei fehlschlägt, wird die Aktivierung abgebrochen. In diesem Fall sollten die Einstellungen der Internetverbindung geprüft werden. Sollte es nicht gelingen, den Fehler zu beheben, wenden Sie sich an den technischen Support.

6. Gehen Sie zur Eingabe des Geheimcodes (s. Abschnitt "Geheimcode eingeben" auf S. 117).

TESTVERSION AKTIVIEREN

Gehen Sie folgendermaßen vor, um eine Testversion von Kaspersky Mobile Security 9.0 zu aktivieren:

1. Gehen Sie auf **Start → Programme**.

2. Wählen Sie **KMS 9.0** und starten Sie das Programm. Verwenden Sie dazu den Stylus oder die mittlere Joystick-Taste.

   Das Fenster **Aktivieren** wird geöffnet.

3. Gehen Sie auf **Testversion**.

4. Bestätigen Sie die Internetverbindung mit **Ja**.

   Das Programm sendet eine Anfrage an den Aktivierungsserver von Kaspersky Lab, lädt eine Schlüsseldatei herunter und installiert sie.

Wenn bei der Verbindung mit dem Aktivierungsserver Fehler aufgetreten sind und keine Schlüsseldatei heruntergeladen wurde, wenden Sie sich an den technischen Support.

5. Gehen Sie zur Eingabe des Geheimcodes (s. Abschnitt "Geheimcode eingeben" auf S. 117).

AKTIVIERUNGSCODE ONLINE KAUFEN

Gehen Sie folgendermaßen vor, um im Online-Shop einen Aktivierungscode zu kaufen:

1. Gehen Sie auf **Start → Programme**.
2. Wählen Sie **KMS 9.0** und starten Sie das Programm. Verwenden Sie dazu den Stylus oder die mittlere Joystick-Taste.

   Das Fenster **Aktivieren** wird geöffnet.
3. Gehen Sie auf **Online kaufen**.

   Das Fenster **Online kaufen** wird geöffnet.
4. Klicken Sie auf **Öffnen**.

   Die Website http://www.kaspersky.com/gotopartnersite/def72/buy wird geöffnet. Hier können Sie ein Formular zur Lizenzverlängerung ausfüllen.
5. Folgen Sie den einzelnen Schritten der Anweisung.
6. Nachdem Sie einen Aktivierungscode gekauft haben, gehen Sie zur Aktivierung einer kommerziellen Programmversion (s. Abschnitt "Kommerzielle Version aktivieren" auf S. 115).

GEHEIMCODE EINGEBEN

Nachdem das Programm aktiviert wurde, werden Sie aufgefordert, einen Geheimcode einzugeben. Der *Geheimcode* verhindert einen unautorisierten Zugriff auf die Programmeinstellungen. Der aktuelle Geheimcode kann später geändert werden.

Der Geheimcode wird in folgenden Fällen abgefragt:

- für den Zugriff auf das Programm
- für den Zugriff auf verschlüsselte Daten
- zur Aktivierung / Deaktivierung der Komponente *Privatsphäre*
- beim Senden eines Befehls mit Hilfe einer speziellen SMS-Nachricht für die Fernsteuerung folgender Funktionen: Blockieren, SMS-Clean, SIM-Watch, GPS-Find, Privatsphäre.
- bei der Deinstallation des Programms

Merken Sie sich den Geheimcode gut. Ohne Geheimcode können die Funktionen von Kaspersky Mobile Security nicht mehr ausgeführt werden, und es ist nicht mehr möglich, auf verschlüsselte Daten zuzugreifen und das Programm zu entfernen.

Ein Geheimcode sollte aus mindestens sieben Ziffern bestehen.

Gehen Sie folgendermaßen vor, um einen Geheimcode einzugeben:

1. Nach der Aktivierung des Programms geben Sie im Feld **Neuen Code eingeben** die Ziffern ein, die Ihren Code bilden.

2. Wiederholen Sie die Eingabe im Feld **Code bestätigen**.

   Ein eingegebener Code wird automatisch auf seine Sicherheit geprüft.

3. Wenn die Prüfung ergibt, dass ein Code unsicher ist, erfolgt eine Warnung, und das Programm erfragt eine Bestätigung. Klicken Sie auf **OK**, um den Code zu verwenden. Klicken Sie auf **Nein**, um einen neuen Code festzulegen.

4. Klicken Sie zum Abschluss auf **OK**.

PROGRAMM STARTEN

Gehen Sie folgendermaßen vor, um Kaspersky Mobile Security 9.0 zu starten:

1. Gehen Sie auf **Start → Programme**.

2. Wählen Sie **KMS 9.0** und starten Sie das Programm. Verwenden Sie dazu den Stylus oder die mittlere Joystick-Taste.

3. Geben Sie den Geheimcode ein und klicken Sie auf **OK**.

Ein Fenster mit dem Schutzstatus von Kaspersky Mobile Security 9.0 wird geöffnet (s. Abschnitt "Fenster für den Schutzstatus" auf S. 124). Klicken Sie auf **Menü**, um zu den Optionen des Programms zu wechseln.

UPDATE DER PROGRAMM-DATENBANKEN

Bei der Suche nach Bedrohungen verwendet Kaspersky Mobile Security 9.0 die Programm-Datenbanken, die eine Beschreibung aller derzeit bekannten schädlichen Programme und entsprechende Desinfektionsmethoden sowie eine Beschreibung sonstiger unerwünschter Objekte enthalten. Die Datenbanken, die zum Lieferumfang von Kaspersky Mobile Security 9.0 gehören, können zum Zeitpunkt der Installation bereits veraltet sein.

Es wird empfohlen, die Datenbanken sofort nach der Programminstallation zu aktualisieren.

Um die Programm-Datenbanken zu aktualisieren, muss auf dem mobilen Gerät eine Internetverbindung eingerichtet sein.

Gehen Sie folgendermaßen vor, um das Update der Programm-Datenbanken zu starten:

1. Gehen Sie auf **Menü → Anti-Virus**.

   Das Fenster **Anti-Virus** wird geöffnet.

2. Gehen Sie auf **Update**.

   Das Fenster **Update** wird geöffnet.

3. Gehen Sie auf **Update**.

Das Programm startet das Update der Datenbanken von einem Kaspersky-Lab-Server. Informationen über den Updatevorgang werden auf dem Bildschirm angezeigt.

GERÄT AUF VIREN UNTERSUCHEN

Es wird empfohlen, Ihr mobiles Gerät nach der Programminstallation vollständig auf schädliche Objekte zu untersuchen.

Die erste Untersuchung erfolgt mit von Kaspersky Lab vordefinierten Einstellungen.

➧ *Gehen Sie folgendermaßen vor, um eine vollständige Untersuchung des Geräts zu starten:*

1. Gehen Sie auf **Menü** → **Anti-Virus**.

   Das Fenster **Anti-Virus** wird geöffnet.

2. Gehen Sie auf **Scan**.

   Das Fenster **Scan** wird geöffnet.

3. Wählen Sie **Alles scannen**.

PROGRAMM-INFO ANZEIGEN

Sie können allgemeine Informationen zum Programm, dessen Version und die Kopierberechtigungen anzeigen.

➧ *Gehen Sie folgendermaßen vor, um Informationen über das Programm anzuzeigen:*

1. Gehen Sie auf **Menü** → **Erweitert**.

   Das Fenster **Erweitert** wird geöffnet.

2. Gehen Sie auf den Punkt **Programm-Infos** (s. Abb. unten).

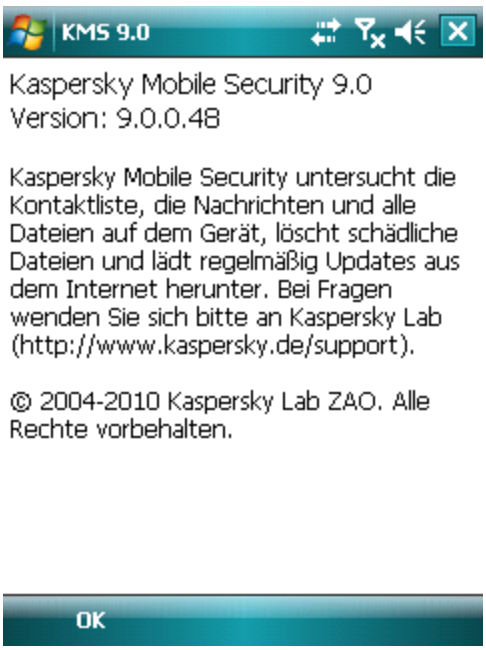

KMS 9.0
Kaspersky Mobile Security 9.0
Version: 9.0.0.48
Kaspersky Mobile Security untersucht die Kontaktliste, die Nachrichten und alle Dateien auf dem Gerät, löscht schädliche Dateien und lädt regelmäßig Updates aus dem Internet herunter. Bei Fragen wenden Sie sich bitte an Kaspersky Lab (http://www.kaspersky.de/support).
© 2004-2010 Kaspersky Lab ZAO. Alle Rechte vorbehalten.
OK

Abbildung 72. Programm-Info

LIZENZVERWALTUNG

Im Zusammenhang mit der Lizenzierung von Kaspersky-Lab-Programmen sind folgende Begriffe wichtig:

- Lizenzvertrag
- Lizenz
- Schlüsseldatei

Diese drei Begriffe sind miteinander verbunden und bilden ein einheitliches Lizenzierungsschema.

Die Begriffe werden im Folgenden ausführlich erklärt.

Dieser Abschnitt informiert außerdem darüber, wie Informationen zur Lizenz von Kaspersky Mobile Security 9.0 angezeigt werden können und wie die Nutzungsdauer der Lizenz verlängert wird.

IN DIESEM ABSCHNITT

Über den Lizenzvertrag 120

Über Lizenzen für Kaspersky Mobile Security 120

Über Schlüsseldateien für Kaspersky Mobile Security 121

Lizenz-Info anzeigen 121

Lizenz verlängern 122

ÜBER DEN LIZENZVERTRAG

Der *Lizenzvertrag* ist ein Vertrag zwischen einer natürlichen oder juristischen Person, die rechtmäßiger Besitzer eines Exemplars von Kaspersky Mobile Security ist, und der Kaspersky Lab ZAO. Der Lizenzvertrag gehört zum Lieferumfang jedes Kaspersky-Lab-Programms. Er legt die Rechte und Einschränkungen für die Nutzung von Kaspersky Mobile Security genau fest.

In Übereinstimmung mit dem Lizenzvertrag erhalten Sie durch den Erwerb und die Installation eines Kaspersky-Lab-Programms das unbefristete Besitzrecht an einer Kopie.

Kaspersky Lab bietet Ihnen folgende Zusatzleistungen an:

- Technischer Support
- Update der Datenbanken für Kaspersky Mobile Security
- Update der Programm-Module von Kaspersky Mobile Security

Um diese Leistungen zu nutzen, sind der Erwerb und die Aktivierung einer Lizenz erforderlich (s. Abschnitt "Über Lizenzen für Kaspersky Mobile Security" auf S. 120).

ÜBER LIZENZEN FÜR KASPERSKY MOBILE SECURITY

Die *Lizenz* verleiht das Recht zur Nutzung von Kaspersky Mobile Security und der zum Programm gehörenden Zusatzleistungen (s. Abschnitt "Über den Lizenzvertrag" auf S. 120), die von Kaspersky Lab und seinen Partnern angeboten werden.

Jede Lizenz wird durch Gültigkeitsdauer und Typ charakterisiert.

Die *Gültigkeitsdauer einer Lizenz* ist die Zeitspanne, für die Ihnen die Zusatzleistungen zur Verfügung stehen. Der Umfang der angebotenen Leistungen ist vom Lizenztyp abhängig.

Es sind folgende Lizenztypen vorgesehen:

Test – kostenlose Lizenz mit beschränkter Gültigkeitsdauer. Eine solche Lizenz dient zum Kennenlernen von Kaspersky Mobile Security. Sie wird zusammen mit einer Testversion des Programms geliefert und besitzt eine kurze Gültigkeitsdauer, während der Sie auf die Wissensdatenbank (http://support.kaspersky.de) und das Forum (http://forum.kaspersky.com/index.php?showforum=77) zugreifen können. Wenn Sie eine Testlizenz verwenden, können Sie den technischen Support nicht nutzen. Nach Ablauf der Gültigkeit stellt Kaspersky Mobile Security seine Funktion ein.

Kommerziell – gekaufte Lizenz, deren Gültigkeitsdauer i.d.R. ein Jahr beträgt. Eine Lizenz dieses Typs erhält der Benutzer beim Kauf des Programms. Nach Ablauf der Gültigkeit einer kommerziellen Lizenz stehen bestimmte Funktionen von Kaspersky Mobile Security nicht mehr zur Verfügung, und die Datenbanken werden nicht mehr aktualisiert. In diesem Fall ist für das Gerät kein umfassender Schutz mehr gewährleistet.

Um das Programm und die Zusatzleistungen zu verwenden, sind der Kauf und die Installation einer kommerziellen Lizenz erforderlich.

Eine Lizenz wird durch die Installation einer Schlüsseldatei aktiviert (s. Abschnitt "Über Schlüsseldateien für Kaspersky Mobile Security" auf S. 121).

ÜBER SCHLÜSSELDATEIEN FÜR KASPERSKY MOBILE SECURITY

Die *Schlüsseldatei* ist eine Datei, die Ihnen als persönlicher Schlüssel dient und für die Arbeit des Programms erforderlich ist. Die Schlüsseldatei realisiert auf technischem Weg die Aktivierung einer ihr entsprechenden Lizenz und damit Ihr Recht zur Nutzung des Programms und der Zusatzleistungen.

Eine Schlüsseldatei wird nach der Eingabe des Aktivierungscodes bei der Aktivierung automatisch übertragen.

Eine Schlüsseldatei enthält folgende Informationen:

- Gültigkeitsdauer der Lizenz
- Typ der Lizenz (Test, kommerziell)
- Lizenzbeschränkungen (z.B. auf welche Anzahl von Geräten sich die Lizenz bezieht).
- Kontaktdaten des technischen Supports
- Gültigkeitsdauer der Schlüsseldatei

Die *Gültigkeitsdauer der Schlüsseldatei* gibt die "Haltbarkeitsdauer" an, die eine Schlüsseldatei bei ihrer Erstellung erhält. Das ist der Zeitraum, nach dessen Ablauf die Schlüsseldatei ungültig wird und die entsprechende Lizenz nicht mehr aktiviert werden kann.

Das folgende Beispiel erklärt das Verhältnis zwischen der Gültigkeitsdauer eines Schlüssels und der Gültigkeitsdauer einer Lizenz.

Beispiel:

Gültigkeitsdauer der Lizenz: 300 Tage

Erstellungsdatum der Schlüsseldatei: 01.09.2009

Gültigkeitsdauer der Schlüsseldatei: 300 Tage

Installationsdatum der Schlüsseldatei (Aktivierung der Lizenz): 10.09.09, d.h. 9 Tage nach dem Erstellungsdatum.

Ergebnis:

Resultierende Gültigkeitsdauer der Lizenz: 300 Tage minus 9 Tage = 291 Tage.

LIZENZ-INFO ANZEIGEN

Sie können folgende Informationen zur Lizenz erhalten: Schlüsseldatei, Typ, Anzahl der verbleibenden Tage und Gerätenummer.

Gehen Sie folgendermaßen vor, um Informationen zur Lizenz anzuzeigen:

1. Gehen Sie auf **Menü** → **Erweitert**.

   Das Fenster **Erweitert** wird geöffnet.

2. Gehen Sie auf den Punkt **Lizenz**.

Das Fenster **Lizenz** wird geöffnet.

3. Wählen Sie **Lizenz-Info**.

LIZENZ VERLÄNGERN

Kaspersky Mobile Security 9.0 erlaubt es, die Programmlizenz zu erneuern.

Eine Lizenz kann auf folgende Weise verlängert werden:

- **Online** – Programm auf einer Website für ein Jahr aktivieren.
- **Mit Aktivierungscode** – Programm mit einem Aktivierungscode aktivieren. Den Aktivierungscode können Sie auf der Seite http://www.kaspersky.de/store oder bei den Vertriebspartnern von Kaspersky Lab erwerben.

Um das Programm zu aktivieren, muss auf dem mobilen Gerät eine Internetverbindung eingerichtet sein.

IN DIESEM ABSCHNITT

Lizenz mit Aktivierungscode verlängern 122

Lizenz online verlängern 123

LIZENZ MIT AKTIVIERUNGSCODE VERLÄNGERN

Gehen Sie folgendermaßen vor, um die Lizenz mit einem Aktivierungscode zu verlängern:

1. Gehen Sie auf **Menü** → **Erweitert**.

   Das Fenster **Erweitert** wird geöffnet.

2. Gehen Sie auf den Punkt **Lizenz**.

   Das Fenster **Lizenz** wird geöffnet.

3. Gehen Sie auf den Punkt **Verlängerung**.

   Das Fenster **Verlängerung** wird geöffnet.

4. Geben Sie den Code in die entsprechenden vier Felder ein und klicken Sie dann auf **Weiter** (s. Abb. unten).

Abbildung 73. Lizenz mit Aktivierungscode verlängern

5. Bestätigen Sie die Internetverbindung mit **Ja**.

   Das Programm sendet eine Anfrage an den Aktivierungsserver von Kaspersky Lab, lädt automatisch eine Schlüsseldatei herunter und installiert sie. Wenn die Installation der Schlüsseldatei erfolgreich verläuft, werden auf dem Bildschirm Informationen über die Lizenz angezeigt.

   Wenn der von Ihnen eingegebene Aktivierungscode ungültig ist, erscheint eine entsprechende Meldung auf dem Bildschirm.

6. Klicken Sie zum Abschluss auf **OK**.

LIZENZ ONLINE VERLÄNGERN

Gehen Sie folgendermaßen vor, um eine Lizenz online zu verlängern:

1. Gehen Sie auf **Menü** → **Erweitert**.

   Das Fenster **Erweitert** wird geöffnet.

2. Gehen Sie auf den Punkt **Lizenz**.

   Das Fenster **Lizenz** wird geöffnet.

3. Gehen Sie auf **Online verlängern**. Der Menüpunkt heißt **Online kaufen**, wenn die Lizenz abgelaufen ist.

   Das Fenster **Online verlängern** wird geöffnet.

4. Klicken Sie auf **Öffnen** (s. Abb. unten).

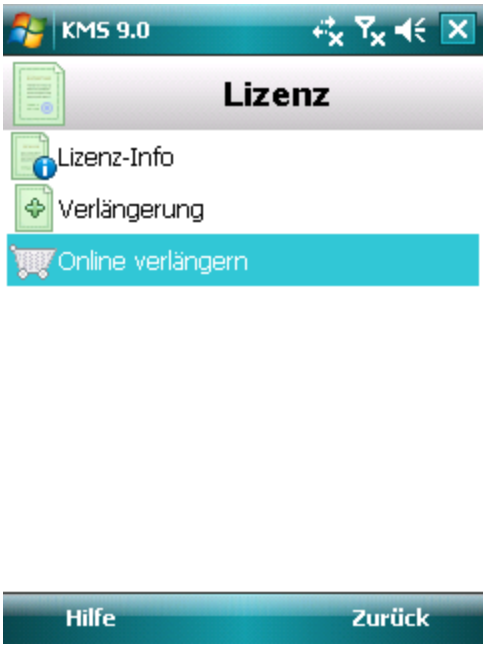


Abbildung 74. Lizenz online verlängern

Es wird eine Website geöffnet, auf der Sie ein Formular zur Verlängerung der Lizenzgültigkeit ausfüllen können.

Wenn die Lizenz abgelaufen ist, öffnet sich die Webseite http://www.kaspersky.com/gotopartnersite/def72/buy, auf der Sie online einen Aktivierungscode kaufen können.

5. Folgen Sie den einzelnen Schritten der Anweisung.

6. Nachdem die Bestellung für die Lizenzverlängerung abgeschlossen wurde, geben Sie den neuen Aktivierungscode ein (s. Abschnitt "Lizenz mit Aktivierungscode verlängern" auf S. 122).

PROGRAMMOBERFLÄCHE

Die Benutzeroberfläche von Kaspersky Mobile Security 9.0 ist intuitiv verständlich und bequem zu handhaben. Dieser Abschnitt informiert über ihre wichtigsten Elemente.

IN DIESEM ABSCHNITT

Fenster für den Schutzstatus.....124

Programm-Menü.....126

FENSTER FÜR DEN SCHUTZSTATUS

Der Status der wichtigsten Programmkomponenten wird im Fenster für den Schutzstatus angezeigt.

Es gibt drei Varianten für den Status. Jeder Status wird durch eine bestimmte Farbe signalisiert. Die Farben entsprechen den Signalen einer Ampel. Grün bedeutet, dass der Schutz Ihres Geräts dem erforderlichen Niveau entspricht. Gelb und Rot signalisieren, dass Sicherheitsrisiken vorliegen. Als Bedrohung gilt nicht nur der Fund schädlicher Programme, sondern auch die Verwendung veralteter Datenbanken, deaktivierte Schutzkomponenten, Auswahl einer niedrigen Sicherheitsstufe u.a.

Das Fenster für den Schutzstatus ist sofort nach dem Programmstart verfügbar und bietet folgende Informationen:

- **Schutz** – Status des Echtzeitschutzes (s. Abschnitt "Schutz für das Dateisystem " auf S. 127).

  Grün bedeutet, dass der Schutz aktiviert ist und dem erforderlichen Niveau entspricht. Die Programm-Datenbanken sind aktuell.

  Gelb zeigt an, dass die Datenbanken seit mehreren Tagen nicht aktualisiert wurden.

  Rot signalisiert Probleme, die zu Datenverlust oder zur Infektion des Geräts führen können. Beispiel: Der Schutz ist deaktiviert. Möglicherweise wurde das Programm längere Zeit nicht aktualisiert.

- **Firewall** – Stufe für den Schutz des Geräts vor unerwünschter Netzwerkaktivität (s. Abschnitt "Filterung der Netzwerkaktivität. Firewall" auf S. 180).

  Das grüne Statussymbol bedeutet, dass die Komponente aktiviert ist. Es wurde eine Sicherheitsstufe für die Firewall ausgewählt.

  Rot zeigt an, dass die Netzwerkaktivität nicht gefiltert wird.

- **Diebstahlschutz** – Status des Datenschutzes für den Fall eines Diebstahls oder Verlusts des Geräts (s. Abschnitt "Datenschutz bei Verlust oder Diebstahl des Geräts" auf S. 160).

  Das grüne Statussymbol bedeutet, dass die Diebstahlschutz-Funktionen, die unter dem Status der Komponente angezeigt werden, aktiviert sind.

  Rot zeigt an, dass alle Funktionen des Diebstahlschutzes deaktiviert sind.

- **Privatsphäre** – Status des Schutzes für vertrauliche Daten (s. Abschnitt "Persönliche Daten verbergen" auf S. 171).

  Das grüne Statussymbol bedeutet, dass die Komponente aktiviert ist. Vertrauliche Daten werden verborgen.

  Gelb warnt davor, dass die Komponente deaktiviert ist. Persönliche Daten werden angezeigt und sind zur Anzeige verfügbar.

- **Lizenz** – Gültigkeitsdauer der Lizenz (s. Abschnitt "Lizenzverwaltung" auf S. 119).

  Das grüne Statussymbol bedeutet, dass die Lizenz noch mehr als 14 Tage gültig ist.

  Gelb warnt davor, dass die Lizenz weniger als 14 Tage gültig ist.

Rot signalisiert, dass die Gültigkeit der Lizenz abgelaufen ist.

Abbildung 75. Fenster Status der Programmkomponenten

Sie können auch in das Fenster für den Schutzstatus wechseln. Wählen Sie dazu **Menü → Schutzstatus**.

PROGRAMM-MENÜ

Die Programmkomponenten sind logisch angeordnet und stehen im Programm-Menü zur Verfügung. Die einzelnen Menüpunkte erlauben es, die Einstellungen einer ausgewählten Komponente zu öffnen oder Schutzaufgaben zu wählen (s. Abb. unten).

Abbildung 76. Programm-Menü

Das Menü von Kaspersky Mobile Security 9.0 enthält folgende Punkte:

- **Anti-Virus** – Virenschutz für das Dateisystem, Untersuchung und Update der Programm-Datenbanken
- **Diebstahlschutz** – Bei Diebstahl oder Verlust das Gerät blockieren und Daten löschen
- **Privatsphäre** – vertrauliche Daten auf dem Gerät verbergen
- **Verschlüsselung** – Datenverschlüsselung zum Schutz der Informationen auf dem Gerät
- **Anti-Spam** – Filterung von unerwünschten eingehenden Anrufen und Nachrichten
- **Kindersicherung** – Kontrolle über ausgehende Anrufe und Nachrichten
- **Firewall** – Netzwerkschutz für das Gerät
- **Erweitert** – allgemeine Programmeinstellungen, Informationen zum Programm, den verwendeten Datenbanken und der Lizenz
- **Schutzstatus** – Informationen über den Schutzstatus des Geräts
- **Beenden** – Programm beenden

➡ *Um das Programm-Menü zu öffnen,*

gehen Sie auf **Menü**.

Verwenden Sie zur Navigation innerhalb des Programm-Menüs den Joystick des Geräts oder den Stylus.

➡ *Gehen Sie folgendermaßen vor, um zum Statusfenster für die Programmkomponenten zurückzukehren:*

gehen Sie auf **Menü → Schutzstatus**.

➡ *Gehen Sie folgendermaßen vor, um das Programm zu beenden:*

gehen Sie auf **Menü → Beenden**.

SCHUTZ FÜR DAS DATEISYSTEM

Dieser Abschnitt informiert über den Schutz, der das Dateisystem Ihres Geräts vor Infektionen schützt. Außerdem wird beschrieben, wie der Schutz aktiviert / angehalten wird und wie die Schutzeinstellungen angepasst werden.

IN DIESEM ABSCHNITT

Schutz 127

Schutz aktivieren / deaktivieren 128

Aktion für gefundene Objekte wählen 129

SCHUTZ

Der Schutz wird beim Hochfahren des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Geräts und untersucht alle Dateien, die geöffnet, gespeichert und gestartet werden. Der Untersuchungsvorgang für eine Datei wird nach folgendem Ablauf ausgeführt:

1. Die Komponente fängt den Zugriff des Benutzers oder eines Programms auf eine beliebige Datei ab.

2. Eine Datei wird auf schädliche Objekte analysiert. Schädliche Objekte werden auf Basis der Programm-Datenbanken erkannt. Die Datenbanken enthalten eine Beschreibung aller momentan bekannten schädlichen Objekte und entsprechende Desinfektionsmethoden.

3. Aufgrund der Analyseergebnisse bestehen folgende Varianten für das Verhalten von Kaspersky Mobile Security 9.0:

   - Wenn in einer Datei Schadcode gefunden wird, sperrt das Programm die Datei und führt die festgelegte Aktion aus.

   - Wenn in einer Datei kein schädlicher Code gefunden wird, erhält der Benutzer sofort Zugriff auf die Datei.

Informationen über die Untersuchungsergebnisse werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. 191).

SCHUTZ AKTIVIEREN / DEAKTIVIEREN

Wenn der Schutz aktiviert ist, werden alle Aktionen in Ihrem System permanent kontrolliert. Der Virenschutz beansprucht die Ressourcen des Geräts. Wenn mehrere Aufgaben ausgeführt werden, kann der Schutz vorübergehend angehalten werden, um die Auslastung des Geräts zu senken.

Die Kaspersky-Lab-Spezialisten warnen ausdrücklich davor, den Schutz zu deaktivieren, da dies zur Infektion Ihres Computers und zu Datenverlust führen kann.

Der aktuelle Schutzstatus wird im Fenster **Anti-Virus** neben dem Menüpunkt **Schutz** angezeigt.

Der Schutz kann folgendermaßen aktiviert / deaktiviert werden:

- aus dem Menü für die Einstellungen der Komponente
- aus dem Menü **Anti-Virus**

Verwenden Sie den Joystick oder die Navigationstasten des Geräts, um die Parameterwerte zu ändern.

➧ *Gehen Sie folgendermaßen vor, um den Schutz zu aktivieren:*

1. Gehen Sie auf **Menü** → **Anti-Virus**.

   Das Fenster **Anti-Virus** wird geöffnet.

2. Gehen Sie auf **Schutz**.

   Das Fenster **Einstellungen** wird geöffnet.

3. Aktivieren Sie das Kontrollkästchen **Schutz aktivieren** (s. Abb. unten).

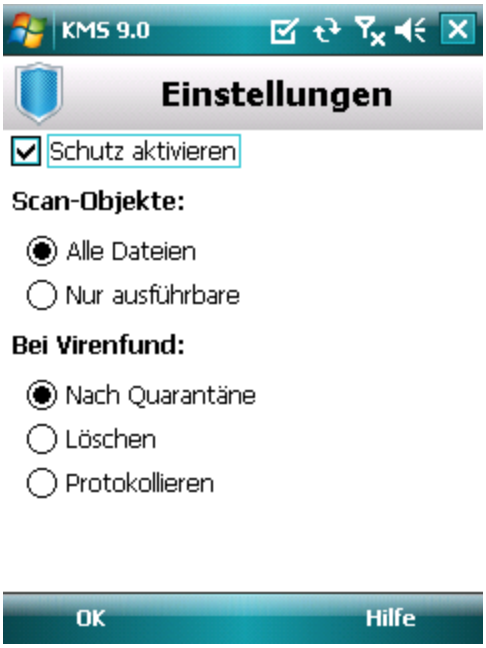


Abbildung 77. Schutz aktivieren

4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

- *Gehen Sie folgendermaßen vor, um den Schutz zu deaktivieren:*

1. Gehen Sie auf **Menü** → **Anti-Virus**.

   Das Fenster **Anti-Virus** wird geöffnet.

2. Gehen Sie auf **Schutz**.

   Das Fenster **Einstellungen** wird geöffnet.

3. Deaktivieren Sie das Kontrollkästchen **Schutz aktivieren**.

4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

- *Gehen Sie folgendermaßen vor, um den Schutz schnell zu aktivieren / deaktivieren:*

1. Gehen Sie auf **Menü** → **Anti-Virus**.

2. Das Fenster **Anti-Virus** wird geöffnet.

3. Klicken Sie auf **Aktivieren** / **Deaktivieren**. Die Beschriftung der Schaltfläche ändert sich abhängig vom aktuellen Schutzstatus in das jeweilige Gegenteil.

AKTION FÜR GEFUNDENE OBJEKTE WÄHLEN

In der Grundeinstellung werden gefundene schädliche Objekte von Kaspersky Mobile Security 9.0 in die Quarantäne verschoben. Die Aktion, die das Programm beim Fund eines schädlichen Objekts ausführen soll, kann geändert werden.

Verwenden Sie den Joystick oder die Navigationstasten des Geräts, um die Parameterwerte zu ändern.

Um die Einstellungen des Schutzes zu ändern, vergewissern Sie sich, dass der Schutz aktiviert ist.

Gehen Sie folgendermaßen vor, um die Reaktion des Programms auf ein schädliches Objekt einzustellen (s. Abb. unten):

1. Gehen Sie auf **Menü** → **Anti-Virus**.

   Das Fenster **Anti-Virus** wird geöffnet.

2. Gehen Sie auf **Schutz**.

   Das Fenster **Einstellungen** wird geöffnet.

3. Legen Sie fest, welche Aktion das Programm beim Fund eines schädlichen Objekts ausführen soll. Wählen Sie dazu einen Wert für **Bei Virenfund** (s. Abb. unten):

   - **Nach Quarantäne** – Objekte in die Quarantäne verschieben
   - **Löschen** – schädliche Objekte löschen, ohne den Benutzer zu benachrichtigen
   - **Protokollieren** – schädliche Objekte überspringen und Fund in den Programmbericht eintragen. Versuche zum Zugriff auf ein Objekt (z.B. Kopieren oder Öffnen) werden blockiert.

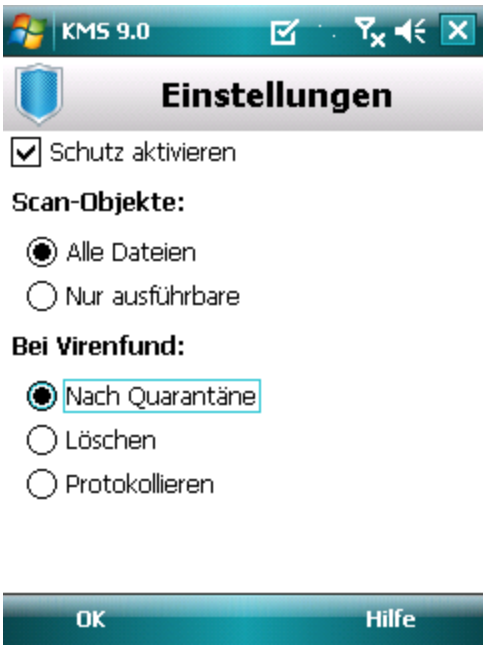


Abbildung 78. Aktion für Objekt wählen

4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

UNTERSUCHUNG DES GERÄTS

Dieser Abschnitt informiert über die Virenuntersuchung. Sie erlaubt es, auf Ihrem Gerät Bedrohungen zu finden und zu neutralisieren. Außerdem werden hier folgende Vorgänge beschrieben: Untersuchungsaufgabe starten, Zeitplan für den Aufgabenstart erstellen, Untersuchungsobjekte wählen, Aktion des Programms für den Fund einer Bedrohung festlegen.

IN DIESEM ABSCHNITT

Über Scan auf Befehl....131

Untersuchung manuell starten....131

Untersuchung nach Zeitplan starten....133

Typ der Untersuchungsobjekte wählen....134

Archiv-Untersuchung anpassen....135

Aktion für gefundene Objekte wählen....136

ÜBER SCAN AUF BEFEHL

Mit der Untersuchung des Geräts lassen sich schädliche Objekte erkennen und neutralisieren. Mit Kaspersky Mobile Security 9.0 kann der Inhalt des Geräts vollständig oder teilweise untersucht werden, d.h. die Untersuchung lässt sich auf den Inhalt des internen Gerätespeichers oder eines bestimmten Ordners (auch eines Ordners auf einer Speicherkarte) beschränken.

Die Untersuchung des Geräts wird nach folgendem Ablauf ausgeführt:

1. Kaspersky Mobile Security 9.0 untersucht Dateien der festgelegten Typen (s. Abschnitt "Typ der Untersuchungsobjekte wählen" auf S. 134).

2. Bei der Untersuchung wird die Datei auf schädliche Objekte analysiert. Schädliche Objekte werden auf Basis der Programm-Datenbanken erkannt. Die Datenbanken enthalten eine Beschreibung aller momentan bekannten schädlichen Objekte und entsprechende Desinfektionsmethoden.

   Aufgrund der Analyseergebnisse bestehen folgende Varianten für das Verhalten von Kaspersky Mobile Security 9.0:

   - Wenn in einer Datei schädlicher Code gefunden wird, sperrt Kaspersky Mobile Security 9.0 die Datei und führt die in den Einstellungen festgelegte Aktion aus (s. Abschnitt "Aktion für gefundene Objekte wählen" auf S. 136).

   - Wenn kein schädlicher Code gefunden wird, wird die Datei sofort zum Zugriff freigegeben.

Eine Untersuchungsaufgabe kann manuell oder automatisch nach einem zuvor erstellten Zeitplan (s. Abschnitt "Untersuchung nach Zeitplan starten" auf S. 133) gestartet werden.

Informationen über die Ergebnisse des Scan auf Befehl werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. 191).

UNTERSUCHUNG MANUELL STARTEN

Sie können eine Untersuchung manuell starten, wenn der Prozessor des Geräts nicht mit anderen Aufgaben beschäftigt ist.

➧ *Gehen Sie folgendermaßen vor, um die Virenuntersuchung manuell zu starten:*

1. Gehen Sie auf **Menü** → **Anti-Virus**.

   Das Fenster **Anti-Virus** wird geöffnet.

2. Gehen Sie auf **Scan**.

Das Fenster **Scan** wird geöffnet.

3. Wählen Sie einen Untersuchungsbereich für das Gerät (s. Abb. unten):

   - **Alles scannen** – das gesamte Dateisystem des Geräts untersuchen. Standardmäßig werden folgende Objekte untersucht: Gerätespeicher und Speicherkarten.

   - **Speicher scannen** – im Systemspeicher laufende Prozesse und die dazu gehörenden Dateien untersuchen.

   - **Ordner scannen** – einzelnes Objekt im Dateisystem des Geräts oder auf einer eingelegten Speicherkarte untersuchen. Durch Klick auf **Ordner scannen** öffnet sich ein Fenster, in dem das Dateisystem des Geräts dargestellt ist. Verwenden Sie zur Navigation im Dateisystem den Joystick oder die Navigationstasten . Um die Untersuchung eines Ordners zu starten, markieren Sie den entsprechenden Ordner und klicken Sie auf **Scannen**.

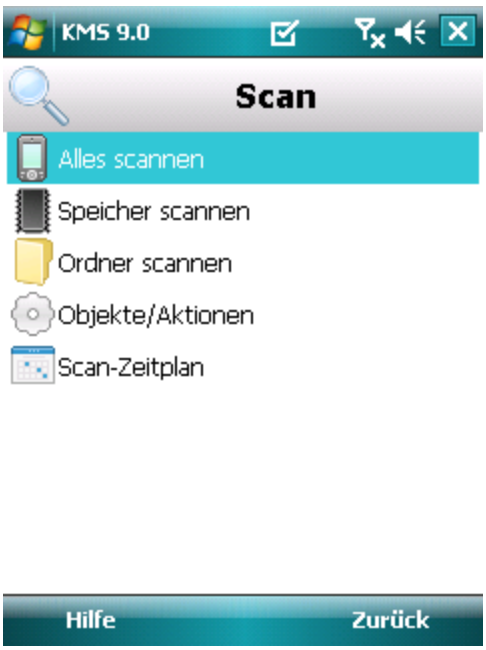


Abbildung 79. Untersuchungsbereich wählen

Nach dem Start der Untersuchung öffnet sich das Untersuchungsfenster (s. Abb. unten), in dem der aktuelle Status angezeigt wird: Anzahl der untersuchten Objekte und Pfad zum Objekt, das gerade untersucht wird.

Abbildung 80. Untersuchungsfenster

Beim Fund eines schädlichen Objekts führt Kaspersky Mobile Security 9.0 die in den Untersuchungseinstellungen festgelegte Aktion aus (s. Abschnitt "Aktion für gefundene Objekte wählen" auf S. 136).

Wenn Kaspersky Mobile Security 9.0 eine Bedrohung findet, verschiebt es diese standardmäßig in die Quarantäne.

Nach Abschluss der Untersuchung erscheint auf dem Bildschirm eine Statistik mit folgendem Inhalt:

- Anzahl der untersuchten Objekte
- Anzahl der gefundenen, unter Quarantäne gestellten und gelöschten Viren
- Anzahl der übersprungenen Objekte (Beispiele: *Datei wird vom Betriebssystem verwendet* oder *Keine ausführbare Datei,* wenn nur ausführbare Dateien untersucht werden).
- Zeitpunkt der Untersuchung

4. Klicken Sie zum Abschluss auf **OK**.

UNTERSUCHUNG NACH ZEITPLAN STARTEN

Mit Kaspersky Mobile Security 9.0 kann ein Zeitplan eingerichtet werden, nach dem die Untersuchung automatisch zur angegebenen Zeit startet. Die Untersuchung erfolgt im Hintergrund. Wenn ein infiziertes Objekt gefunden wird, führt das Programm die Aktion aus, die in den Untersuchungseinstellungen festgelegt wurde (s. Abschnitt "Aktion für gefundene Objekte wählen" auf S. 136).

Die Untersuchung nach Zeitplan ist standardmäßig deaktiviert.

➡ *Gehen Sie folgendermaßen vor, um einen Zeitplan für die Untersuchung anzupassen:*

1. Gehen Sie auf **Menü** → **Anti-Virus**.

   Das Fenster **Anti-Virus** wird geöffnet.

2. Gehen Sie auf **Scan**.

   Das Fenster **Scan** wird geöffnet.

3. Gehen Sie auf **Scan-Zeitplan**.

   Das Fenster **Zeitplan** wird geöffnet.

4. Aktivieren Sie das Kontrollkästchen **Scan nach Zeitplan** (s. Abb. unten).

5. Wählen Sie einen Wert für **Frequenz**:

   - **Täglich**: Die Untersuchung erfolgt jeden Tag. Geben Sie im Eingabefeld die **Zeit** ein.
   - **Wöchentlich**: Die Untersuchung erfolgt einmal pro Woche. Geben Sie **Zeit** und **Wochentag** an.

Abbildung 81. Automatischen Start der Untersuchung anpassen

6. Klicken Sie auf **OK**, um die Änderungen zu speichern.

TYP DER UNTERSUCHUNGSOBJEKTE WÄHLEN

Sie können festlegen welche Objekttypen auf Schadcode untersucht werden sollen.

Verwenden Sie den Joystick oder die Navigationstasten des Geräts, um die Parameterwerte zu ändern.

Gehen Sie folgendermaßen vor, um Untersuchungsobjekte zu wählen:

1. Gehen Sie auf **Menü** → **Anti-Virus**.

   Das Fenster **Anti-Virus** wird geöffnet.

2. Gehen Sie auf **Scan**.

   Das Fenster **Scan** wird geöffnet.

3. Gehen Sie auf **Objekte / Aktionen**.

Das Fenster **Objekte / Aktionen** wird geöffnet.

4. Wählen Sie im Block **Scan-Objekte** die zu scannenden Objekte (s. Abb. unten):

   - **Alle Dateien** – alle Dateitypen untersuchen. Es werden Archive der folgenden Formaten gescannt: *.zip, *.sis, *.cab und *.sisx.

   - **Nur ausführbare** – nur ausführbare Programmdateien folgender Formate untersuchen: *.exe, *.dll, *.sis, *.mdl, *.app, * .rdl, *.prt, *.pxt, *.ldd, *.pdd, *.class. Dabei werden Archive nicht entpackt und nicht untersucht.

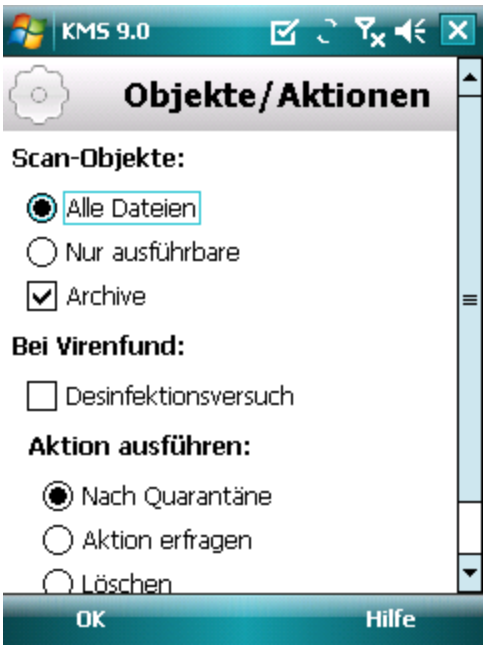


Abbildung 82. Schutzobjekte wählen

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

ARCHIV-UNTERSUCHUNG ANPASSEN

Viren werden häufig in Archiven versteckt. Um den Inhalt von Archiven zu untersuchen, müssen diese entpackt werden. Das kann sich negativ auf die Leistungsfähigkeit des Geräts auswirken.

In der Grundeinstellung ist das Entpacken von Archiven aktiviert. Das Programm scannt Archive der folgenden Formate: *.zip, *.sis, *.sisx, *.cab. Um die Untersuchung zu beschleunigen, können Sie das Entpacken von Archiven ausschalten.

Verwenden Sie den Joystick oder die Navigationstasten des Geräts, um die Parameterwerte zu ändern.

➧ *Gehen Sie folgendermaßen vor, um das Entpacken von Archiven zu deaktivieren:*

1. Gehen Sie auf **Menü** → **Anti-Virus**.

   Das Fenster **Anti-Virus** wird geöffnet.

2. Gehen Sie auf **Scan**.

   Das Fenster **Scan** wird geöffnet.

3. Gehen Sie auf **Objekte / Aktionen**.

Das Fenster **Objekte / Aktionen** wird geöffnet.

4. Deaktivieren Sie im Block **Scan-Objekte** das Kontrollkästchen **Archive**.

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

AKTION FÜR GEFUNDENE OBJEKTE WÄHLEN

In der Grundeinstellung werden gefundene infizierte Objekte von Kaspersky Mobile Security 9.0 in die Quarantäne verschoben. Die Aktion, die das Programm beim Fund eines schädlichen Objekts ausführen soll, kann geändert werden.

Verwenden Sie den Joystick oder die Navigationstasten des Geräts, um die Parameterwerte zu ändern.

Gehen Sie folgendermaßen vor, um die Reaktion des Programms auf ein schädliches Objekt einzustellen (s. Abb. unten):

1. Gehen Sie auf **Menü** → **Anti-Virus**.

   Das Fenster **Anti-Virus** wird geöffnet.

2. Gehen Sie auf **Scan**.

   Das Fenster **Scan** wird geöffnet.

3. Gehen Sie auf **Objekte / Aktionen**.

   Das Fenster **Objekte / Aktionen** wird geöffnet.

4. Damit das Programm versucht, infizierte Objekte zu desinfizieren, aktivieren Sie für **Bei Virenfund** das Kontrollkästchen **Desinfektionsversuch** (s. Abb. unten).

5. Legen Sie eine Aktion für gefundene schädliche Objekte fest. Wählen Sie dazu einen Wert für **Aktion ausführen**:

   Wenn das Kontrollkästchen **Desinfektionsversuch** aktiviert ist, heißt dieser Parameter **Wenn irreparabel**. Dieser Parameter legt fest, welche Aktion das Programm ausführen soll, wenn sich ein Objekt nicht desinfizieren lässt.

   - **Nach Quarantäne** – Objekte in die Quarantäne verschieben
   - **Aktion erfragen** – beim Fund von schädlichen Objekten den Benutzer nach einer Aktion fragen
   - **Löschen** – schädliche Objekte löschen, ohne den Benutzer zu benachrichtigen

- **Protokollieren** – schädliche Objekte überspringen und Fund in den Programmbericht eintragen. Versuche zum Zugriff auf ein Objekt (z.B. Kopieren oder Öffnen) werden blockiert.

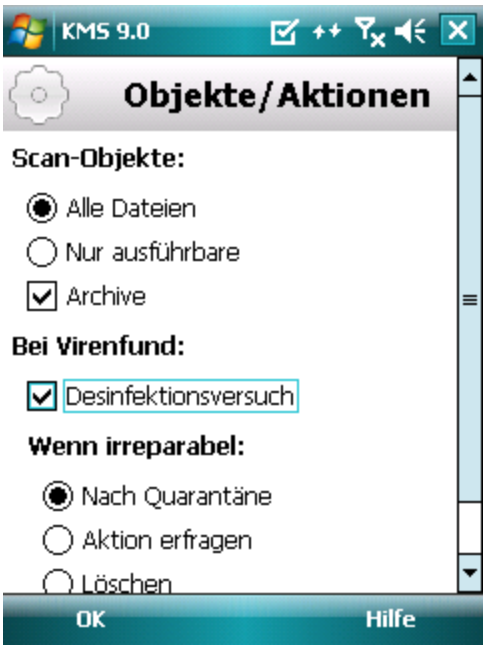


Abbildung 83. Aktion für schädliches Objekt wählen

6. Klicken Sie auf **OK**, um die Änderungen zu speichern.

QUARANTÄNE FÜR SCHÄDLICHE OBJEKTE

Dieser Abschnitt informiert über den speziellen Speicher *Quarantäne*, in den potentiell gefährliche Objekte verschoben werden. Außerdem wird hier die Arbeit mit Quarantäneobjekten beschrieben: Quarantäneobjekte anzeigen, wiederherstellen oder löschen.

IN DIESEM ABSCHNITT

Quarantäne....137

Quarantäneobjekte anzeigen....138

Quarantäneobjekte wiederherstellen....138

Quarantäneobjekte löschen....139

QUARANTÄNE

Die Quarantäne ist ein spezieller Ordner, in den Kaspersky Mobile Security 9.0 potentiell gefährliche Objekte verschiebt.

Bei einer Untersuchung des Geräts oder im Rahmen des Echtzeit-Schutzes können schädliche Objekte erkannt und unter Quarantäne gestellt werden.

Die in die Quarantäne verschobenen Objekte werden in gepackter Form gespeichert, sodass deren Aktivierung ausgeschlossen ist und von ihnen keine Gefahr mehr für das Gerät ausgeht. Die Objekte können später gelöscht oder wiederhergestellt werden.

QUARANTÄNEOBJEKTE ANZEIGEN

Sie können die Objekte, die in die Quarantäne verschoben wurden, anzeigen. Für jedes Objekt werden der vollständige Name und das Funddatum angezeigt.

- *Gehen Sie folgendermaßen vor, um eine Liste der Quarantäneobjekte anzuzeigen:*

1. Gehen Sie auf **Menü** → **Anti-Virus**.

   Das Fenster **Anti-Virus** wird geöffnet.

2. Gehen Sie auf **Quarantäne**.

   Das Fenster **Quarantäne** wird geöffnet. Es enthält eine Liste der Quarantäneobjekte (s. Abb. unten).

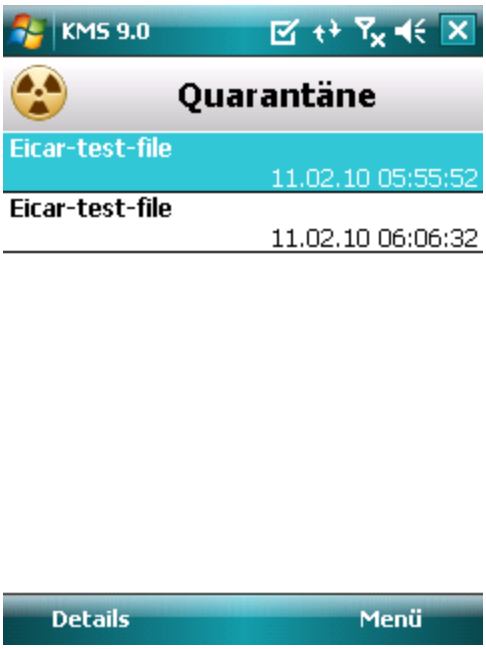


Abbildung 84. Liste der Quarantäneobjekte

QUARANTÄNEOBJEKTE WIEDERHERSTELLEN

Wenn Sie sicher sind, dass ein gefundenes Objekt keine Gefahr für das Gerät darstellt, können Sie es aus der Quarantäne wiederherstellen. Ein wiederhergestelltes Objekt wird in den ursprünglichen Ordner verschoben.

- *Gehen Sie folgendermaßen vor, um ein Objekt aus der Quarantäne wiederherzustellen:*

1. Gehen Sie auf **Menü** → **Anti-Virus**.

   Das Fenster **Anti-Virus** wird geöffnet.

2. Gehen Sie auf **Quarantäne**.

   Das Fenster **Quarantäne** wird geöffnet.

3. Wählen Sie ein Objekt, das wiederhergestellt werden soll, und gehen Sie dann auf **Menü** → **Wiederherstellen**.

Das markierte Objekt wird aus der Quarantäne im ursprünglichen Ordner wiederhergestellt.

QUARANTÄNEOBJEKTE LÖSCHEN

Es können ein oder alle Elemente, die in der Quarantäne gespeichert sind, gelöscht werden.

- *Gehen Sie folgendermaßen vor, um ein Objekt aus der Quarantäne zu löschen:*

1. Gehen Sie auf **Menü** → **Anti-Virus**.

   Das Fenster **Anti-Virus** wird geöffnet.

2. Gehen Sie auf **Quarantäne**.

   Das Fenster **Quarantäne** wird geöffnet.

3. Wählen Sie ein zu löschendes Objekt und klicken Sie dann auf **Menü** → **Löschen**.

Das markierte Objekt wird aus der Quarantäne gelöscht.

- *Gehen Sie folgendermaßen vor, um alle Quarantäneobjekte zu löschen:*

1. Gehen Sie auf **Menü** → **Anti-Virus**.

   Das Fenster **Anti-Virus** wird geöffnet.

2. Gehen Sie auf **Quarantäne**.

   Das Fenster **Quarantäne** wird geöffnet.

3. Klicken Sie auf **Menü** → **Alle löschen**.

Alle Quarantäneobjekte werden gelöscht.

EINGEHENDE ANRUFE UND SMS-NACHRICHTEN FILTERN

Dieser Abschnitt informiert über die Komponente *Anti-Spam*, die eingehende Nachrichten und Anrufe aufgrund einer Schwarzen und Weißen Liste filtert. Außerdem werden hier folgende Vorgänge beschrieben: Schwarze und Weiße Liste anlegen, in Anti-Spam eine Aktion für eingehende Nachrichten und Anrufe festlegen, Komponente anpassen.

IN DIESEM ABSCHNITT

Anti-Spam 140

Über die Modi für Anti-Spam 141

Anti-Spam-Modus ändern 141

Schwarze Liste anlegen 142

Weiße Liste anlegen 145

Reaktion auf SMS-Nachrichten und Anrufe von Kontakten, die nicht im Telefonbuch stehen 148

Reaktion auf SMS-Nachrichten von Nicht-Ziffern-Nummern 149

Aktion für eingehende SMS-Nachrichten wählen 150

Aktion für eingehende Anrufe wählen 151

ANTI-SPAM

Anti-Spam schützt das Gerät vor unerwünschten Nachrichten und Anrufen. Anti-Spam filtert eingehende SMS-Nachrichten und Anrufe unter Verwendung einer Schwarzen und Weißen Liste.

Die Listen bestehen aus Einträgen. Jeder Eintrag kann folgende Parameter enthalten:

- Datentyp (SMS-Nachricht, Anruf, SMS-Nachricht und Anruf), auf den die Filterung angewendet wird (obligatorischer Parameter)
- Telefonnummer, von der die Daten stammen
- Text, den eine SMS-Nachricht enthalten kann

Anti-Spam filtert SMS-Nachrichten und Anrufe gemäß den festgelegten Einstellungen (s. Abschnitt "Über die Modi für Anti-Spam" auf S. 141). Nach diesen Einstellungen untersucht Anti-Spam alle eingehenden Anrufe und SMS-Nachrichten und stuft sie als erwünscht oder unerwünscht (Spam) ein. Sobald Anti-Spam einen Anruf oder eine SMS als erwünscht oder unerwünscht einstuft, wird die Untersuchung abgeschlossen.

Der Algorithmus für Anti-Spam umfasst standardmäßig folgende Schritte:

1. Untersuchung einer eingehenden SMS-Nachricht auf Übereinstimmung mit Telefonnummer und Text:
   a. Nach der Schwarzen Liste. Wenn die Liste einen Eintrag enthält, dessen Nummer und Text mit den Daten aus der eingehenden SMS-Nachricht übereinstimmen, wird die SMS-Nachricht als unerwünscht eingestuft und blockiert. Das Programm löscht die blockierte SMS-Nachricht.
   b. Nach der Weißen Liste. Wenn die Liste einen Eintrag enthält, dessen Nummer und Text mit den Daten aus der eingehenden SMS-Nachricht übereinstimmen, wird die SMS-Nachricht als erwünscht eingestuft und erlaubt.
2. Ein Anruf oder eine SMS-Nachricht wird nur auf Übereinstimmung mit einer Nummer untersucht:
   a. Nach der Schwarzen Liste. Wenn die Liste einen Eintrag enthält, dessen Nummer mit der Nummer des Absenders/Anrufers übereinstimmt, wird der Anruf oder die SMS als Spam eingestuft und blockiert. Das Programm löscht die blockierte SMS-Nachricht.
   b. Nach der Weißen Liste. Wenn die Liste einen Eintrag enthält, dessen Nummer mit der Nummer des Absenders/Anrufers übereinstimmt (wobei im Eintrag kein Text angegeben ist), wird der Anruf oder die SMS als erwünscht eingestuft und erlaubt.
3. Eine Nachricht wird nur auf Übereinstimmung mit einem Text untersucht:
   a. Nach der Schwarzen Liste. Wenn die Liste einen Eintrag enthält, dessen Text mit den Daten aus der eingehenden SMS-Nachricht übereinstimmt (wobei im Eintrag keine Nummer angegeben ist), wird die SMS-Nachricht als Spam eingestuft und blockiert. Das Programm löscht die blockierte SMS-Nachricht.
   b. Nach der Weißen Liste. Wenn die Liste einen Eintrag enthält, dessen Text mit den Daten aus der eingehenden SMS-Nachricht übereinstimmt (wobei im Eintrag keine Nummer angegeben ist), wird die SMS-Nachricht als erwünscht eingestuft und erlaubt.
4. Aktion wählen. Wenn keine Übereinstimmung mit der Schwarzen oder Weißen Liste besteht, werden Anrufe und SMS-Nachrichten in der Grundeinstellung von Anti-Spam erlaubt und im Meldungsfenster erfolgt eine Aktionsabfrage für Anrufe / Nachrichten. Außerdem enthält die Meldung folgende Zusatzinformationen: Für einen angenommenen Anruf wird die Nummer des Anrufers genannt. Für SMS-Nachrichten werden Telefonnummer und Nachrichteninhalt angegeben.

Informationen über blockierte SMS-Nachrichten und Anrufe werden in einem Bericht erfasst (s. Abschnitt "Programmberichte" auf S. 191).

ÜBER DIE MODI FÜR ANTI-SPAM

Ein Modus von Anti-Spam basiert auf einer Auswahl von Parametern, nach denen Ihr Gerät vor unerwünschten Meldungen und Anrufen geschützt wird.

Es sind folgende Modi für Anti-Spam vorgesehen:

- **Aus** – alle SMS-Nachrichten und Anrufe werden erlaubt. Anti-Spam deaktivieren.
- **Weiße Liste** – SMS-Nachrichten und Anrufe von Nummern, die auf der Weißen Liste stehen, werden erlaubt. Alle übrigen SMS-Nachrichten und Anrufe werden blockiert. Blockierte SMS-Nachrichten werden gelöscht.
- **Schwarze Liste** – SMS-Nachrichten und Anrufe von Nummern, die auf der Schwarzen Liste stehen, werden blockiert. Blockierte SMS-Nachrichten werden gelöscht. Alle übrigen SMS-Nachrichten und Anrufe werden erlaubt.
- **Beide Listen** – eingehende SMS-Nachrichten und Anrufe werden mit der Schwarzen und Weißen Liste gefiltert. Geht eine SMS-Nachricht oder ein Anruf von einer Telefonnummer ein, die nicht auf einer Liste steht, dann werden Sie von Anti-Spam benachrichtigt. Sie können die SMS oder den Anruf blockieren oder erlauben und die Telefonnummer in die Schwarze oder Weiße Liste aufnehmen. Dieser Modus ist standardmäßig aktiviert.

Sie können den Modus für Anti-Spam ändern (s. Abschnitt "Anti-Spam-Modus ändern" auf S. 141). Der aktuelle Modus von Anti-Spam wird im Fenster **Anti-Spam** neben dem Menüpunkt **Modus** angezeigt.

ANTI-SPAM-MODUS ÄNDERN

Gehen Sie folgendermaßen vor, um einen Modus für Anti-Spam zu wählen:

1. Gehen Sie auf **Menü** → **Anti-Spam**.

   Das Fenster **Anti-Spam** wird geöffnet.

2. Gehen Sie auf **Modus**.

   Das Fenster **Modus** wird geöffnet.

3. Wählen Sie dazu einen Wert für **Anti-Spam-Modus** (s. Abb. unten).

Abbildung 85. Anti-Spam-Modus ändern

4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

SCHWARZE LISTE ANLEGEN

Sie können eine Schwarze Liste anlegen, nach der Anti-Spam eingehende SMS-Nachrichten und Anrufe blockieren soll.

Die Liste enthält Telefonnummern und Phrasen, deren Vorhandensein in einer SMS-Nachricht darauf hindeuten, dass es sich um Spam handelt.

Informationen über blockierte SMS-Nachrichten und Anrufe werden in einem Bericht erfasst (s. Abschnitt "Programmberichte" auf S. 191).

IN DIESEM ABSCHNITT

Eintrag zur Schwarzen Liste hinzufügen 142

Eintrag der Schwarzen Liste ändern 144

Eintrag aus Schwarzer Liste löschen 145

EINTRAG ZUR SCHWARZEN LISTE HINZUFÜGEN

Beachten Sie, dass eine Nummer nicht gleichzeitig auf der Schwarzen und Weißen Liste der Telefonnummern für Anti-Spam stehen kann. Wenn eine Nummer bereits in einer der Listen vorhanden ist, zeigt Kaspersky Mobile Security 9.0 eine entsprechende Meldung an.

➧ *Um der Schwarzen Liste für Anti-Spam einen Eintrag hinzuzufügen:*

1. Gehen Sie auf **Menü** → **Anti-Spam**.

Das Fenster **Anti-Spam** wird geöffnet.

2. Gehen Sie auf **Schwarze Liste**.

   Das Fenster **Schwarze Liste** wird geöffnet.

3. Gehen Sie auf **Menü** → **Hinzufügen** (s. Abb. unten).

   Das Fenster **Neuer Eintrag** wird geöffnet.

Abbildung 86. Eintrag zur Schwarzen Liste hinzufügen

4. Nehmen Sie folgende Einstellungen vor (s. Abb. unten):

   - **Eingehende verbieten** – Typ der eingehenden Informationen, der von Anti-Spam für eine Nummer blockiert werden soll:
     - **Anrufe und SMS** – eingehende SMS-Nachrichten und Anrufe blockieren.
     - **Nur Anrufe** – nur eingehende Anrufe blockieren.
     - **Nur SMS** - nur eingehende SMS-Nachrichten blockieren.
   - **Telefonnummer** – Telefonnummer, von der SMS-Nachrichten und / oder Anrufen blockiert werden sollen. Die Nummer kann mit einer Ziffer, mit einem Buchstaben oder mit dem Zeichen "+" beginnen und darf Ziffern / Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "*" und "?" möglich (wobei "*" für eine beliebige Zeichenfolge steht und "?" für ein beliebiges Einzelzeichen).

- **Mit Text** – Schlüsselwörter / Phrasen, die darauf hinweisen, dass es sich bei einer empfangenen SMS-Nachricht um Spam handelt. Diese Option ist nur verfügbar, wenn der Parameter **Eingehende verbieten** den Wert **Nur SMS** besitzt.

Abbildung 87. Parameter eines Eintrags

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

EINTRAG DER SCHWARZEN LISTE ÄNDERN

Alle Parameterwerte der Einträge aus der Schwarzen Liste für verbotene Nummern können geändert werden.

Um einen Eintrag in der Schwarzen Liste für Anti-Spam zu ändern:

1. Gehen Sie auf **Menü** → **Anti-Spam**.

   Das Fenster **Anti-Spam** wird geöffnet.

2. Gehen Sie auf **Schwarze Liste**.

   Das Fenster **Schwarze Liste** wird geöffnet.

3. Wählen Sie aus der Liste ein Element, das geändert werden soll, und gehen Sie dann auf **Menü** → **Ändern**.

   Das Fenster **Einträg ändern** wird geöffnet.

4. Ändern Sie die erforderlichen Parameter:

   - **Eingehende verbieten** – Typ der eingehenden Informationen, der von Anti-Spam für eine Nummer blockiert werden soll:

     - **Anrufe und SMS** – eingehende SMS-Nachrichten und Anrufe blockieren.
     - **Nur Anrufe** – nur eingehende Anrufe blockieren.
     - **Nur SMS** - nur eingehende SMS-Nachrichten blockieren.

- **Telefonnummer** – Telefonnummer, von der SMS-Nachrichten und / oder Anrufen blockiert werden sollen. Die Nummer kann mit einer Ziffer, mit einem Buchstaben oder mit dem Zeichen "+" beginnen und darf Ziffern / Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "*" und "?" möglich (wobei "*" für eine beliebige Zeichenfolge steht und "?" für ein beliebiges Einzelzeichen).

- **Mit Text** – Schlüsselwörter / Phrasen, die darauf hinweisen, dass es sich bei einer empfangenen SMS-Nachricht um Spam handelt. Diese Option ist nur verfügbar, wenn der Parameter **Eingehende verbieten** den Wert **Nur SMS** besitzt.

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

EINTRAG AUS SCHWARZER LISTE LÖSCHEN

Es kann vorkommen, dass eine Nummer versehentlich zur Schwarzen Liste der verbotenen Nummern hinzugefügt wurde. Eine solche Nummer kann aus der Liste gelöscht werden. Außerdem können Sie die Schwarze Liste von Anti-Spam leeren, d.h. alle Einträge daraus löschen.

Um einen Eintrag aus der Schwarzen Liste für Anti-Spam zu löschen:

1. Gehen Sie auf **Menü** → **Anti-Spam**.

   Das Fenster **Anti-Spam** wird geöffnet.

2. Gehen Sie auf **Schwarze Liste**.

   Das Fenster **Schwarze Liste** wird geöffnet.

3. Markieren Sie den zu löschenden Eintrag in der Liste und gehen Sie dann auf **Menü** → **Löschen**.

4. Bestätigen Sie das Löschen des Eintrags Klicken Sie dazu auf **Ja**.

Um die Schwarze Liste für Anti-Spam zu leeren:

1. Gehen Sie auf **Menü** → **Anti-Spam**.

   Das Fenster **Anti-Spam** wird geöffnet.

2. Gehen Sie auf **Schwarze Liste**.

   Das Fenster **Schwarze Liste** wird geöffnet.

3. Gehen Sie auf **Optionen** → **Alle löschen**.

Die Liste wird geleert.

WEISSE LISTE ANLEGEN

Sie können eine Weiße Liste anlegen, nach der Anti-Spam eingehende SMS-Nachrichten und Anrufe erlauben soll.

Die Liste enthält Telefonnummern von Absendern und Phrasen, von denen kein Spam erwartet wird.

IN DIESEM ABSCHNITT

Eintrag zur Weißen Liste hinzufügen 146

Eintrag der Weißen Liste ändern 147

Eintrag aus Weißer Liste löschen 148

EINTRAG ZUR WEISSEN LISTE HINZUFÜGEN

Beachten Sie, dass eine Nummer nicht gleichzeitig auf der Schwarzen und Weißen Liste der Telefonnummern für Anti-Spam stehen kann. Wenn eine Nummer bereits in einer der Listen vorhanden ist, zeigt Kaspersky Mobile Security 9.0 eine entsprechende Meldung an.

Um der Weißen Liste für Anti-Spam einen Eintrag hinzuzufügen:

1. Gehen Sie auf **Menü** → **Anti-Spam**.

   Das Fenster **Anti-Spam** wird geöffnet.

2. Gehen Sie auf **Weiße Liste**.

   Das Fenster **Weiße Liste** wird geöffnet.

3. Gehen Sie auf **Menü** → **Hinzufügen** (s. Abb. unten).

   Das Fenster **Neuer Eintrag** wird geöffnet.

Abbildung 88. Eintrag zur Weißen Liste hinzufügen

4. Nehmen Sie folgende Einstellungen vor (s. Abb. unten):

   - **Eingehende erlauben** – Typ der eingehenden Informationen, der von Anti-Spam für eine Nummer erlaubt werden soll:

     - **Anrufe und SMS** – eingehende Anrufe und SMS-Nachrichten erlauben.
     - **Nur Anrufe** – nur eingehende Anrufe erlauben.
     - **Nur SMS** - nur eingehende SMS-Nachrichten erlauben.

   - **Telefonnummer** – Telefonnummer, für die der Empfang von SMS-Nachrichten bzw. von Anrufen zugelassen wird. Die Nummer kann mit einer Ziffer, mit einem Buchstaben oder mit dem Zeichen "+" beginnen und darf Ziffern / Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "*" und "?" möglich (wobei "*" für eine beliebige Zeichenfolge steht, "?" für ein beliebiges Einzelzeichen).

- **Mit Text** – Schlüsselwörter/Phrasen, die darauf hinweisen, dass es sich bei einer empfangenen SMS-Nachricht nicht um Spam handelt. Diese Option ist nur verfügbar, wenn der Parameter **Eingehende erlauben** den Wert **Nur SMS** besitzt.

Abbildung 89. Parameter eines Eintrags

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

EINTRAG DER WEISSEN LISTE ÄNDERN

Alle Parameterwerte der Einträge aus der Weißen Liste für erlaubte Nummern können geändert werden.

Um einen Eintrag in der Weißen Liste für Anti-Spam zu ändern:

1. Gehen Sie auf **Menü** → **Anti-Spam**.

   Das Fenster **Anti-Spam** wird geöffnet.

2. Gehen Sie auf **Weiße Liste**.

   Das Fenster **Weiße Liste** wird geöffnet.

3. Wählen Sie aus der Liste ein Element, das geändert werden soll, und gehen Sie dann auf **Menü** → **Ändern**.

   Das Fenster **Einträg ändern** wird geöffnet.

4. Ändern Sie die erforderlichen Parameter:

   - **Eingehende erlauben** – Typ der eingehenden Informationen, der von Anti-Spam für eine Nummer erlaubt werden soll:
     - **Anrufe und SMS** – eingehende Anrufe und SMS-Nachrichten erlauben.
     - **Nur Anrufe** – nur eingehende Anrufe erlauben.
     - **Nur SMS** - nur eingehende SMS-Nachrichten erlauben.

- **Telefonnummer** – Telefonnummer, für die der Empfang von SMS-Nachrichten bzw. von Anrufen zugelassen wird. Die Nummer kann mit einer Ziffer, mit einem Buchstaben oder mit dem Zeichen "+" beginnen und darf Ziffern / Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "*" und "?" möglich (wobei "*" für eine beliebige Zeichenfolge steht, "?" für ein beliebiges Einzelzeichen).

- **Mit Text** – Schlüsselwörter/Phrasen, die darauf hinweisen, dass es sich bei einer empfangenen SMS-Nachricht nicht um Spam handelt. Diese Option ist nur verfügbar, wenn der Parameter **Eingehende erlauben** den Wert **Nur SMS** besitzt.

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

EINTRAG AUS WEISSER LISTE LÖSCHEN

Sie können einen Eintrag löschen oder die Weiße Liste vollständig leeren.

Um einen Eintrag aus der Weißen Liste für Anti-Spam zu löschen:

1. Gehen Sie auf **Menü** → **Anti-Spam**.

   Das Fenster **Anti-Spam** wird geöffnet.

2. Gehen Sie auf **Weiße Liste**.

   Das Fenster **Weiße Liste** wird geöffnet.

3. Markieren Sie den zu löschenden Eintrag in der Liste und gehen Sie dann auf **Menü** → **Löschen**.

4. Bestätigen Sie das Löschen des Eintrags Klicken Sie dazu auf **Ja**.

Um die Weiße Liste für Anti-Spam zu leeren:

1. Gehen Sie auf **Menü** → **Anti-Spam**.

   Das Fenster **Anti-Spam** wird geöffnet.

2. Gehen Sie auf **Weiße Liste**.

   Das Fenster **Weiße Liste** wird geöffnet.

3. Gehen Sie auf **Optionen** → **Alle löschen**.

Die Liste wird geleert.

REAKTION AUF SMS-NACHRICHTEN UND ANRUFE VON KONTAKTEN, DIE NICHT IM TELEFONBUCH STEHEN

Im Modus **Beide Listen** oder **Weiße Liste** (s. Abschnitt "Über die Modi für Anti-Spam" auf S. 141) können Sie zusätzlich festlegen, wie Anti-Spam auf SMS-Nachrichten und Anrufe von Nummern reagieren soll, die sich nicht in den Kontakten befinden. Die Weiße Liste von Anti-Spam lässt sich durch die Aufnahme der Nummern aus den Kontakten erweitern.

Verwenden Sie den Joystick oder die Navigationstasten des Geräts, um die Parameterwerte zu ändern.

Gehen Sie folgendermaßen vor, um festzulegen, wie Anti-Spam auf eine Nummer reagieren soll, die nicht im Telefonbuch des Geräts steht:

1. Gehen Sie auf **Menü** → **Anti-Spam**.

   Das Fenster **Anti-Spam** wird geöffnet.

2. Gehen Sie auf **Modus**.

3. Das Fenster **Modus** wird geöffnet.

4. Wählen Sie einen Wert für **Kontakte erlauben** (s. Abb. unten):

   - Damit Anti-Spam die Nummern des Telefonbuchs als zusätzliche Weiße Liste betrachtet und SMS-Nachrichten und Anrufe von Nummern blockiert, die nicht im Telefonbuch stehen, aktivieren Sie das Kontrollkästchen **Kontakte erlauben**.

   - Damit Anti-Spam SMS-Nachrichten und Anrufe nur nach dem festgelegten Anti-Spam-Modus filtert, deaktivieren Sie das Kontrollkästchen **Kontakte erlauben**.

Abbildung 90. Reaktion von Anti-Spam auf Nummern, die nicht zu den Kontakten gehören

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

REAKTION AUF SMS-NACHRICHTEN VON NICHT-ZIFFERN-NUMMERN

Im Modus **Beide Listen** oder **Schwarze Liste** (s. Abschnitt "Anti-Spam-Modus ändern" auf S. 141) können Sie die Schwarze Liste durch Aufnahme aller Nicht-Ziffern-Nummern (Nummern, die Buchstaben enthalten) erweitern. In diesem Fall blockiert Anti-Spam den Empfang von SMS-Nachrichten, die von Nicht-Ziffern-Nummern stammen.

Verwenden Sie den Joystick oder die Navigationstasten des Geräts, um die Parameterwerte zu ändern.

Gehen Sie folgendermaßen vor, um festzulegen, wie Anti-Spam auf eingehende SMS-Nachrichten von Nicht-Ziffern-Nummern reagieren soll:

1. Gehen Sie auf **Menü** → **Anti-Spam**.

   Das Fenster **Anti-Spam** wird geöffnet.

2. Gehen Sie auf **Modus**.

   Das Fenster **Modus** wird geöffnet.

3. Wählen Sie einen Wert für den Parameter **Nicht-Ziffern-Nummern blockieren** (s. Abb. unten):

   - Damit Anti-Spam Nachrichten mit Nicht-Ziffern-Nummern automatisch löscht, aktivieren Sie das Kontrollkästchen **Nicht-Ziffern-Nummern blockieren**.

   - Damit Anti-Spam Nachrichten von Nicht-Ziffern-Nummern nur auf Basis des gewählten Anti-Spam-Modus filtert, deaktivieren Sie das Kontrollkästchen **Nicht-Ziffern-Nummern blockieren**.

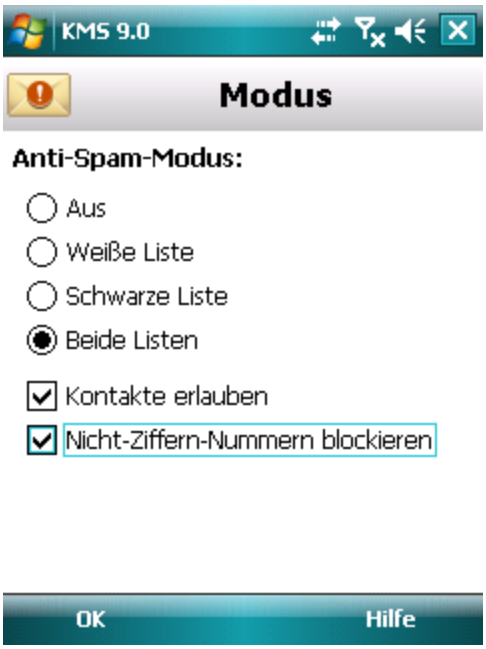


Abbildung 91. Aktion von Anti-Spam für eingehende SMS-Nachrichten von Nicht-Ziffern-Nummern anpassen

4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

AKTION FÜR EINGEHENDE SMS-NACHRICHTEN WÄHLEN

Als Standardmodus für Anti-Spam gilt **Beide Listen** (s. Abschnitt "Über die Modi für Anti-Spam" auf S. 141). Anti-Spam prüft eingehende SMS-Nachrichten auf Übereinstimmungen mit der Schwarzen und Weißen Liste.

Wenn die Nummer des Absenders auf keiner der beiden Listen steht, werden Sie von Anti-Spam darüber informiert. Sie können wählen, welche der vorgeschlagenen Aktionen Anti-Spam mit der eingehenden SMS-Nachricht ausführen soll (s. Abb. unten).

Abbildung 92. Meldung von Anti-Spam über den Empfang einer Nachricht

Sie können eine der folgenden Aktionen für eine SMS-Nachricht wählen:

- Um eine SMS-Nachricht zu blockieren und die Telefonnummer des Absenders in die Schwarze Liste aufzunehmen, wählen Sie **Menü → Zur Schwarzen Liste**.
- Um eine SMS-Nachricht zu erlauben und die Telefonnummer des Absenders in die Weiße Liste aufzunehmen, wählen Sie **Menü → Zur Weißen Liste**.
- Um eine SMS-Nachricht zu erlauben und die Telefonnummer des Absenders in keine der Listen einzutragen, wählen Sie **Überspringen**.

Informationen über blockierte Nachrichten werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. 191).

AKTION FÜR EINGEHENDE ANRUFE WÄHLEN

Als Standardmodus für Anti-Spam gilt **Beide Listen** (s. Abschnitt "Über die Modi für Anti-Spam" auf S. 141). Anti-Spam prüft eingehende Anrufe nach der Schwarzen und Weißen Liste.

Wenn die Nummer des Absenders auf keiner der beiden Listen steht, werden Sie von Anti-Spam nach Gesprächsende darüber informiert, und Sie können eine Aktion für den eingehenden Anruf wählen (s. Abb. unten).

Abbildung 93. Meldung von Anti-Spam über einen angenommenen Anruf

Für eine Nummer, von der ein Anruf erfolgte, können Sie eine der folgenden Aktionen wählen:

- Um die Telefonnummer des Anrufers in die Schwarze Liste aufzunehmen, wählen Sie **Menü → Zur Schwarzen Liste**.
- Um die Telefonnummer des Anrufers in die Weiße Liste aufzunehmen, wählen Sie **Menü → Zur Weißen Liste**.
- Damit die Telefonnummer des Anrufers in keine der Listen eingetragen wird, wählen Sie **Überspringen**.

Informationen über blockierte Anrufe werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. 103).

AUSGEHENDE ANRUFE UND SMS-NACHRICHTEN EINSCHRÄNKEN

Dieser Abschnitt informiert über die Komponente *Kindersicherung,* mit der ausgehende Anrufe und SMS-Nachrichten an bestimmte Nummern eingeschränkt werden können. Außerdem werden hier folgende Vorgänge beschrieben: Liste für erlaubte und verbotene Nummern anlegen, Kindersicherung anpassen.

IN DIESEM ABSCHNITT

Kindersicherung....153

Modi der Kindersicherung....153

Kindersicherung aktivieren / deaktivieren....153

Schwarze Liste anlegen....154

Weiße Liste anlegen....157

KINDERSICHERUNG

Die Komponente *Kindersicherung* filtert ausgehende SMS-Nachrichten und Anrufe nach einer Schwarzen und Weißen Nummernliste.

Wird mindestens eine Übereinstimmung festgestellt, so erfolgt keine weitere Untersuchung. Eine ausgehende SMS-Nachricht oder ein ausgehender Anruf, die/der einem Element der Schwarzen Liste entspricht, wird gesperrt. Bei einer Übereinstimmung mit der Weißen Liste wird der Vorgang erlaubt.

Die Kindersicherung sperrt nur SMS-Nachrichten, die mit Hilfe der Standardmittel des Geräts gesendet werden. Das Blockieren erstreckt sich nicht auf SMS-Nachrichten, die mit Programmen von Drittherstellern gesendet werden.

Informationen über die Arbeit der Komponente werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. 191).

MODI DER KINDERSICHERUNG

Der Modus der Kindersicherung basiert auf einer Auswahl von Parametern, nach denen der Schutz Ihres Geräts vor unerwünschten SMS-Nachrichten und Anrufen ausgeführt wird.

Es sind die folgenden Optionen für die Kindersicherung vorgesehen:

- **Aus** – Kindersicherung deaktivieren. Ausgehende SMS-Nachrichten und Anrufe werden nicht gefiltert.

  Dieser Modus ist standardmäßig aktiviert.

- **Weiße Liste** – SMS-Nachrichten und / oder Anrufe werden nur an Nummern aus der Weißen Liste erlaubt (s. Abschnitt "Weiße Liste anlegen" auf S. 157). Alle übrigen Nachrichten und Anrufe blockiert.

- **Schwarze Liste** – SMS-Nachrichten und / oder Anrufe werden nur an Nummern aus der Schwarzen Liste verboten (s. Abschnitt "Schwarze Liste anlegen" auf S. 154). Alle übrigen Nachrichten und Anrufe werden erlaubt.

Sie können den Modus der Kindersicherung ändern (s. Abschnitt "Kindersicherung aktivieren / deaktivieren" auf S. 153). Der aktuelle Modus der Kindersicherung wird im Fenster **Kindersicherung** neben dem Menüpunkt **Modus** angezeigt.

KINDERSICHERUNG AKTIVIEREN / DEAKTIVIEREN

Gehen Sie folgendermaßen vor, um einen Modus für die Kindersicherung zu ändern:

1. Gehen Sie auf **Menü** → **Kindersicherung**.
2. Das Fenster **Kindersicherung** wird geöffnet.

3. Gehen Sie auf **Modus**.

   Das Fenster **Modus** wird geöffnet.

4. Wählen Sie einen Modus für die Kindersicherung (s. Abb. unten).

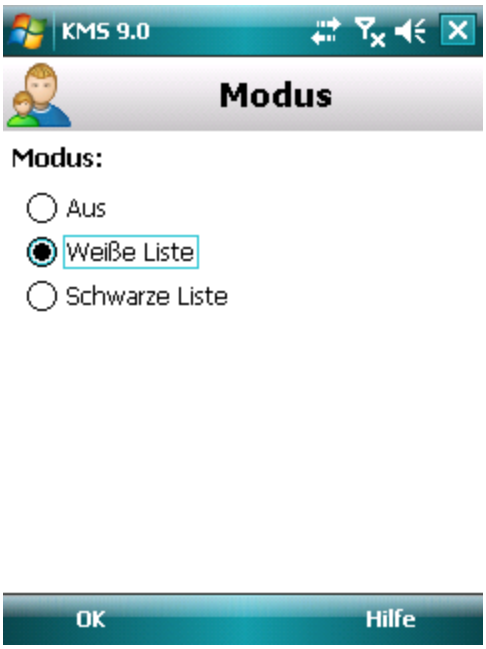


Abbildung 94. Modus für die Kindersicherung ändern

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

SCHWARZE LISTE ANLEGEN

Sie können eine Schwarze Liste anlegen, nach der die Kindersicherung ausgehende SMS-Nachrichten und Anrufe blockieren soll. Die Liste enthält Telefonnummern, an die ausgehende SMS-Nachrichten und Anrufe verboten werden.

Informationen über blockierte SMS-Nachrichten und Anrufe werden in einem Programmbericht (s. Abschnitt "Programmberichte" auf S. 191).

IN DIESEM ABSCHNITT

Eintrag zur Schwarzen Liste hinzufügen 154

Eintrag der Schwarzen Liste ändern 156

Eintrag aus Schwarzer Liste löschen 157

EINTRAG ZUR SCHWARZEN LISTE HINZUFÜGEN

Beachten Sie, dass eine Nummer nicht gleichzeitig auf der Schwarzen und Weißen Nummernliste der Kindersicherung stehen kann. Wenn eine Nummer bereits in einer der Listen vorhanden ist, zeigt Kaspersky Mobile Security 9.0 eine entsprechende Meldung an.

Um der Schwarzen Liste der Kindersicherung einen Eintrag hinzuzufügen:

1. Gehen Sie auf **Menü** → **Kindersicherung**.
2. Das Fenster **Kindersicherung** wird geöffnet.
3. Gehen Sie auf **Schwarze Liste**.

   Das Fenster **Schwarze Liste** wird geöffnet.
4. Gehen Sie auf **Menü** → **Hinzufügen** (s. Abb. unten).

Abbildung 95. Eintrag zur Schwarzen Liste hinzufügen

Das Fenster **Neuer Eintrag** wird geöffnet.

5. Legen Sie die Werte für folgende Parameter fest (s. Abb. unten):

   - **Ausgehende verbieten** – Typ der ausgehenden Informationen, der von der Kindersicherung für eine Nummer blockiert werden soll:
     - **Anrufe und SMS** – ausgehende SMS-Nachrichten und Anrufe blockieren.
     - **Nur Anrufe** – nur ausgehende Anrufe blockieren.
     - **Nur SMS** - nur ausgehende SMS-Nachrichten blockieren.

- **Telefonnummer** – Telefonnummer, für die der Versand von SMS-Nachrichten und/oder Anrufe gesperrt wird. Die Nummer kann mit einer Ziffer, mit einem Buchstaben oder mit dem Zeichen "+" beginnen und darf Ziffern / Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "*" und "?" möglich (wobei "*" für eine beliebige Zeichenfolge steht und "?" für ein beliebiges Einzelzeichen).

Abbildung 96. Parameter eines Eintrags

6. Klicken Sie auf **OK**, um die Änderungen zu speichern.

EINTRAG DER SCHWARZEN LISTE ÄNDERN

Alle Parameterwerte der Einträge aus der Schwarzen Liste für verbotene Nummern können geändert werden.

Um einen Eintrag in der Schwarzen Liste der Kindersicherung zu ändern:

1. Gehen Sie auf **Menü** → **Kindersicherung**.
2. Das Fenster **Kindersicherung** wird geöffnet.
3. Gehen Sie auf **Schwarze Liste**.

   Das Fenster **Schwarze Liste** wird geöffnet.
4. Wählen Sie aus der Liste ein Element, das geändert werden soll, und gehen Sie dann auf **Menü** → **Ändern**.

   Das Fenster **Einträg ändern** wird geöffnet.
5. Ändern Sie die erforderlichen Parameter:

   - **Ausgehende verbieten** – Typ der ausgehenden Informationen, der von der Kindersicherung für eine Nummer blockiert werden soll:
     - **Anrufe und SMS** – ausgehende SMS-Nachrichten und Anrufe blockieren.
     - **Nur Anrufe** – nur ausgehende Anrufe blockieren.
     - **Nur SMS** - nur ausgehende SMS-Nachrichten blockieren.

- **Telefonnummer** – Telefonnummer, für die der Versand von SMS-Nachrichten und/oder Anrufe gesperrt wird. Die Nummer kann mit einer Ziffer, mit einem Buchstaben oder mit dem Zeichen "+" beginnen und darf Ziffern / Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "*" und "?" möglich (wobei "*" für eine beliebige Zeichenfolge steht und "?" für ein beliebiges Einzelzeichen).

6. Klicken Sie auf **OK**, um die Änderungen zu speichern.

EINTRAG AUS SCHWARZER LISTE LÖSCHEN

Es kann vorkommen, dass eine Nummer versehentlich zur Schwarzen Liste der verbotenen Nummern hinzugefügt wurde. Eine solche Nummer kann aus der Liste gelöscht werden. Außerdem können Sie die Schwarze Liste der Kindersicherung leeren, d.h. alle Einträge daraus löschen.

Um einen Eintrag aus der Schwarzen Liste der Kindersicherung zu löschen:

1. Gehen Sie auf **Menü** → **Kindersicherung**.
2. Das Fenster **Kindersicherung** wird geöffnet.
3. Gehen Sie auf **Schwarze Liste**.

   Das Fenster **Schwarze Liste** wird geöffnet.
4. Markieren Sie den zu löschenden Eintrag in der Liste und gehen Sie dann auf **Menü** → **Löschen**.
5. Bestätigen Sie das Löschen. Klicken Sie dazu auf **Ja**.

Um die Schwarze Liste für Anti-Spam zu leeren:

1. Gehen Sie auf **Menü** → **Kindersicherung**.
2. Das Fenster **Kindersicherung** wird geöffnet.
3. Gehen Sie auf **Schwarze Liste**.

   Das Fenster **Schwarze Liste** wird geöffnet.
4. Gehen Sie auf **Optionen** → **Alle löschen**.

Die Liste wird geleert.

WEISSE LISTE ANLEGEN

Sie können eine Weiße Liste anlegen, nach der Anti-Spam eingehende SMS-Nachrichten und Anrufe erlauben soll.

Die Liste enthält Telefonnummern von Absendern und Phrasen, von denen kein Spam erwartet wird.

IN DIESEM ABSCHNITT

Eintrag zur Weißen Liste hinzufügen 158

Eintrag der Weißen Liste ändern 159

Eintrag aus Weißer Liste löschen 160

EINTRAG ZUR WEISSEN LISTE HINZUFÜGEN

Beachten Sie, dass eine Nummer nicht gleichzeitig auf der Schwarzen und Weißen Nummernliste der Kindersicherung stehen kann. Wenn eine Nummer bereits in einer der Listen vorhanden ist, zeigt Kaspersky Mobile Security 9.0 eine entsprechende Meldung an.

Um der Weißen Liste der Kindersicherung einen Eintrag hinzuzufügen:

1. Gehen Sie auf **Menü** → **Kindersicherung**.
2. Das Fenster **Kindersicherung** wird geöffnet.
3. Gehen Sie auf **Weiße Liste**.
4. Das Fenster **Weiße Liste** wird geöffnet.
5. Gehen Sie auf **Menü** → **Hinzufügen** (s. Abb. unten).

Abbildung 97. Eintrag zur Weißen Liste hinzufügen

Das Fenster **Neuer Eintrag** wird geöffnet.

6. Legen Sie die Werte für folgende Parameter fest (s. Abb. unten):

   - **Ausgehende erlauben** – Typ der ausgehenden Informationen, der von der Kindersicherung für eine Nummer erlaubt werden soll:
     - **Anrufe und SMS** – eingehende Anrufe und SMS-Nachrichten erlauben.
     - **Nur Anrufe** – nur ausgehende Anrufe erlauben.
     - **Nur SMS** – nur ausgehende SMS-Nachrichten erlauben.

- **An Telefonnummer** – Telefonnummer, an die Kindersicherung ausgehende SMS-Nachrichten / Anrufe erlauben soll. Die Nummer kann mit einer Ziffer, mit einem Buchstaben oder mit dem Zeichen "+" beginnen und darf Ziffern / Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "*" und "?" möglich (wobei "*" für eine beliebige Zeichenfolge steht, "?" für ein beliebiges Einzelzeichen).

Abbildung 98. Parameter eines Eintrags

7. Klicken Sie auf **OK**, um die Änderungen zu speichern.

EINTRAG DER WEISSEN LISTE ÄNDERN

Alle Parameterwerte der Einträge aus der Weißen Liste für erlaubte Nummern können geändert werden.

Um einen Eintrag in der Weißen Liste der Kindersicherung zu ändern:

1. Gehen Sie auf **Menü** → **Kindersicherung**.
2. Das Fenster **Kindersicherung** wird geöffnet.
3. Gehen Sie auf **Weiße Liste**.
4. Das Fenster **Weiße Liste** wird geöffnet.
5. Wählen Sie aus der Liste ein Element, das geändert werden soll, und gehen Sie dann auf **Menü** → **Ändern**.

   Das Fenster **Einträg ändern** wird geöffnet.
6. Ändern Sie die erforderlichen Parameter:

   - **Ausgehende erlauben** – Typ der ausgehenden Informationen, der von der Kindersicherung für eine Nummer erlaubt werden soll:
     - **Anrufe und SMS** – eingehende Anrufe und SMS-Nachrichten erlauben.
     - **Nur Anrufe** – nur ausgehende Anrufe erlauben.
     - **Nur SMS** – nur ausgehende SMS-Nachrichten erlauben.

- **An Telefonnummer** – Telefonnummer, an die die Kindersicherung ausgehende SMS-Nachrichten / Anrufe erlauben soll. Die Nummer kann mit einer Ziffer, mit einem Buchstaben oder mit dem Zeichen "+" beginnen und darf Ziffern / Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "*" und "?" möglich (wobei "*" für eine beliebige Zeichenfolge steht, "?" für ein beliebiges Einzelzeichen).

7. Klicken Sie auf **OK**, um die Änderungen zu speichern.

EINTRAG AUS WEISSER LISTE LÖSCHEN

Sie können einen Eintrag löschen oder die Weiße Liste vollständig leeren.

Um einen Eintrag aus der Weißen Liste der Kindersicherung zu löschen:

1. Gehen Sie auf **Menü** → **Kindersicherung**.
2. Das Fenster **Kindersicherung** wird geöffnet.
3. Gehen Sie auf **Weiße Liste**.
4. Das Fenster **Weiße Liste** wird geöffnet.
5. Markieren Sie den zu löschenden Eintrag in der Liste und gehen Sie dann auf **Menü** → **Löschen**.
6. Bestätigen Sie das Löschen. Klicken Sie dazu auf **Ja**.

Um die Weiße Liste für Anti-Spam zu leeren:

1. Gehen Sie auf **Menü** → **Kindersicherung**.
2. Das Fenster **Kindersicherung** wird geöffnet.
3. Gehen Sie auf **Weiße Liste**.
4. Das Fenster **Weiße Liste** wird geöffnet.
5. Gehen Sie auf **Optionen** → **Alle löschen**.

Die Liste wird geleert.

DATENSCHUTZ BEI VERLUST ODER DIEBSTAHL DES GERÄTS

Dieser Abschnitt informiert über die Komponente *Diebstahlschutz*, die bei Diebstahl oder Verlust des Geräts einen komplexen Schutz für persönliche Daten bietet und das Auffinden des Geräts erleichtert. Außerdem werden hier folgende Vorgänge beschrieben: Diebstahlschutz aktivieren / deaktivieren, Diebstahlschutz anpassen, Schutz bei Diebstahl oder Verlust des Geräts ferngesteuert starten.

IN DIESEM ABSCHNITT

Diebstahlschutz 161

Gerät blockieren 162

Persönliche Daten löschen 163

Liste der zu löschenden Daten erstellen 166

Wechsel der SIM-Karte auf dem Gerät überwachen 167

Geografische Koordinaten des Geräts ermitteln 168

Diebstahlschutz-Funktionen ferngesteuert starten 170

DIEBSTAHLSCHUTZ

Der Diebstahlschutz schützt die Daten, die auf dem Gerät gespeichert sind, vor unbefugtem Zugriff. Diese Funktion ist von Vorteil, wenn das Gerät verloren geht oder gestohlen wird. Der Diebstahlschutz erlaubt es, per Fernsteuerung ein Gerät zu blockieren und die darauf gespeicherten Daten zu löschen.

Die Komponente umfasst folgende Funktionen:

- Mit der Funktion **SMS-Block** kann das Gerät auf Befehl des Benutzers blockiert werden, und der Benutzer kann einen Text eingeben, der auf dem Display des blockierten Geräts angezeigt wird.
- Die Funktion **SMS-Clean** ermöglicht es, persönliche Benutzerdaten (alle Kontakte, Nachrichten, Galerie, Kalender, Berichte, Netzwerkeinstellungen) aus dem Gerät sowie Daten von Speicherkarten und Dateien aus bestimmten Ordnern unwiderruflich zu löschen.
- **SIM-Watch** erlaubt es, an eine vorgegebene Telefonnummer und / oder E-Mail-Adresse die neue Telefonnummer zu schicken und das Gerät zu sperren, wenn die SIM-Karte gewechselt oder das Gerät ohne SIM eingeschaltet wird.
- **GPS-Find** kann die geografischen Koordinaten des Geräts ermitteln und diese Daten per SMS an das anfragende Gerät oder an eine vorgegebene E-Mail-Adresse senden.

  Diese Funktion eignet sich nur für Geräte mit integriertem GPS-Empfänger.

Für die Verwendung der einzelnen Diebstahlschutz-Funktionen ist der Geheimcode erforderlich, der beim ersten Start von Kaspersky Mobile Security 9.0 festgelegt wurde.

Alle Diebstahlschutz-Funktionen sind nach der Installation von Kaspersky Mobile Security 9.0 zunächst deaktiviert.

Außerdem lassen sich die Diebstahlschutz-Funktionen von Kaspersky Mobile Security 9.0 durch SMS-Befehle an das vermisste / gestohlene Gerät starten (s. Abschnitt "Diebstahlschutz-Funktionen ferngesteuert starten" auf S. 170).

Der aktuelle Status der einzelnen Funktionen wird im Fenster **Diebstahlschutz** neben dem der jeweiligen Funktion angezeigt.

Informationen über die Arbeit der Komponente werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. 191).

GERÄT BLOCKIEREN

Wenn das Gerät vermisst wird oder gestohlen wurde, kann der Zugriff auf die im Gerät gespeicherten Daten mit der ferngesteuerten Funktion SMS-Block gesperrt werden. Das Gerät kann nur durch Eingabe des Geheimcodes entsperrt werden.

Diese Funktion blockiert das Gerät nicht, sondern aktiviert nur die Option für das ferngesteuerte Blockieren.

Um die Blockierfunktion zu aktivieren, gehen Sie folgendermaßen vor:

1. Gehen Sie auf **Menü** → **Diebstahlschutz**.

   Das Fenster **Diebstahlschutz** wird geöffnet.

2. Gehen Sie auf **SMS-Block**.

   Das Fenster **SMS-Block** wird geöffnet.

3. Aktivieren Sie das Kontrollkästchen **SMS-Block aktivieren**.

4. Ändern Sie im Feld **Text beim Blockieren** den Text, der auf dem Display des blockierten Geräts angezeigt werden soll (s. Abb. unten). In der Grundeinstellung wird für die Meldung ein Standardtext verwendet, dem Sie die Nummer des Telefonbesitzers hinzufügen können.

Abbildung 99. Einstellungen der Funktion SMS-Block

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Ein vermisstes Gerät, auf dem die Funktion SMS-Block aktiviert ist, kann auf folgende Weise gesperrt werden:

- Mit der Funktion **Befehl senden**. Dafür ist ein anderes Gerät erforderlich, auf dem Kaspersky Mobile Security 9.0 installiert ist. Auf dem Zweitgerät wird mit Kaspersky Mobile Security 9.0 eine spezielle SMS-Nachricht erstellt und an das verlorene Gerät gesendet. Sie enthält die Telefonnummer des zu blockierenden Geräts und seinen Geheimcode. Der Empfang der speziellen SMS bleibt auf dem zu blockierenden Gerät unbemerkt.

- Mit den Standardfunktionen zum Erstellen einer SMS-Nachricht. Dazu wird auf dem anderen Gerät eine SMS-Nachricht, die aus einem speziellen Text und dem Geheimcode des zu blockierenden Geräts besteht, erstellt und an das verlorene Gerät gesendet.

Um ein Gerät per Fernzugriff zu blockieren, wird die sichere Methode mit der Funktion **Befehl senden** empfohlen. In diesem Fall werden Befehl und Geheimcode in verschlüsselter Form gesendet.

Gehen Sie folgendermaßen vor, um einen Befehl an das vermisste / gestohlene Gerät zu senden:

1. Gehen Sie auf **Menü** → **Erweitert**.

   Das Fenster **Erweitert** wird geöffnet.

2. Gehen Sie auf **Befehl senden**.

   Das Fenster **Befehl senden** wird geöffnet.

3. Setzen Sie den Parameter **Funktion** auf **Gerät blockieren** (s. Abb. unten).

4. Geben Sie im Feld **Telefonnummer** die Telefonnummer des Geräts ein, das blockiert werden soll.

5. Geben Sie im Feld **Remote-Code** den Geheimcode des Geräts ein, an das die Nachricht gerichtet ist.

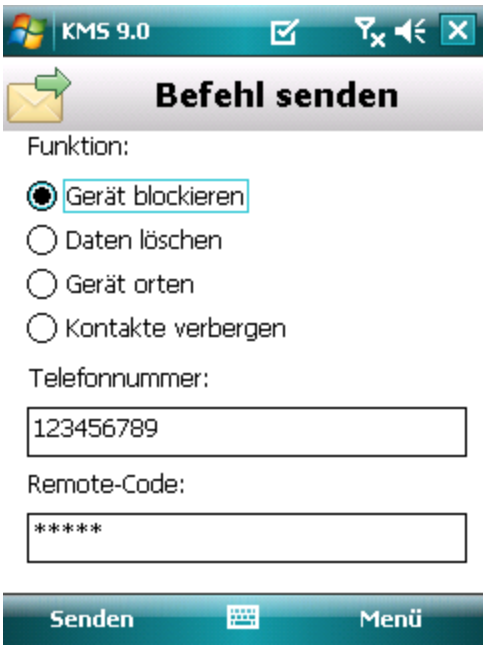


Abbildung 100. Gerät per Fernsteuerung blockieren

6. Klicken Sie auf **Senden**.

Um mit Hilfe der Standardfunktionen eines Handys eine SMS zu erstellen,

schicken Sie an das zu blockierende Gerät eine SMS mit dem Text `block:<Code>` (wobei `<Code>` der Geheimcode des zu blockierenden Geräts ist). Groß- und Kleinschreibung von Buchstaben sowie Leerzeichen vor und nach dem Doppelpunkt sind irrelevant.

PERSÖNLICHE DATEN LÖSCHEN

Bei Diebstahl oder Verlust des mobilen Geräts können mit der Funktion SMS-Clean folgende darauf gespeicherten Informationen gelöscht werden:

- persönliche Benutzerdaten (alle Kontakte, Nachrichten, Galerie, Kalender und Netzwerkeinstellungen). Dabei löscht der Diebstahlschutz die Kontakte, die sich im Telefonbuch des Geräts und auf der SIM-Karte befinden.
- Daten auf Speicherkarten
- Daten im Ordner Eigene Dateien und in anderen festgelegten Ordnern

Das Aktivieren dieser Funktion löscht die auf dem Gerät gespeicherten Daten nicht sofort, sondern aktiviert zunächst nur eine Option zur Datenlöschung.

Der Diebstahlschutz löscht die Daten, die durch die Liste der zu löschenden Objekte festgelegt werden (s. Abschnitt "Liste der zu löschenden Objekte erstellen" auf S. 166) erst dann, wenn das Gerät eine spezielle SMS empfängt.

Gehen Sie folgendermaßen vor, um die Funktion SMS-Clean zu aktivieren:

1. Gehen Sie auf **Menü** → **Diebstahlschutz**.

   Das Fenster **Diebstahlschutz** wird geöffnet.

2. Gehen Sie auf **SMS-Clean**.

   Das Fenster **SMS-Clean** wird geöffnet.

3. Gehen Sie auf **Modus**.

   Das Fenster **SMS-Clean** wird geöffnet.

4. Aktivieren Sie das Kontrollkästchen **SMS-Clean aktivieren**.

5. Wählen Sie den Typ der zu löschenden Daten. Aktivieren Sie dazu im Block **Löschen** die entsprechenden Kontrollkästchen (s. Abb. unten):

   - Aktivieren Sie das Kontrollkästchen **Persönliche Daten**, damit persönliche Daten gelöscht werden.
   - Aktivieren Sie das Kontrollkästchen **Ordner**, damit Dateien aus dem Ordner Eigene Dateien und aus anderen festgelegten Ordnern gelöscht werden.

Abbildung 101. Typ der zu löschenden Daten wählen

6. Klicken Sie auf **OK**, um die Änderungen zu speichern.

7. Erstellen Sie eine Liste der zu löschenden Daten (s. Abschnitt "Liste der zu löschenden Daten erstellen" auf S. 166).

Wenn die Funktion aktiviert ist, können persönliche Daten auf folgende Weise vom Gerät gelöscht werden:

- Mit der Funktion **Befehl senden**. Dafür ist ein anderes Gerät erforderlich, auf dem Kaspersky Mobile Security 9.0 installiert ist. Auf dem Zweitgerät wird mit Kaspersky Mobile Security 9.0 eine spezielle SMS-Nachricht erstellt und an das verlorene Gerät gesendet. Sie enthält die Telefonnummer des Geräts und seinen Geheimcode. Der Empfang einer speziellen SMS bleibt auf dem vermissten / gestohlenen Gerät unbemerkt.

- Mit den Standardfunktionen zum Erstellen einer SMS-Nachricht. Auf dem anderen Gerät wird eine SMS-Nachricht, die aus einem speziellen Text und dem Geheimcode des vermissten/gestohlenen Geräts besteht, erstellt und gesendet.

Um persönliche Daten per Fernsteuerung zu löschen, wird die sichere Methode mit der Funktion Befehl senden empfohlen. In diesem Fall werden Befehl und Geheimcode in verschlüsselter Form gesendet.

Gehen Sie folgendermaßen vor, um einen Befehl an das vermisste / gestohlene Gerät zu senden:

1. Gehen Sie auf **Menü** → **Erweitert**.

   Das Fenster **Erweitert** wird geöffnet.

2. Gehen Sie auf **Befehl senden**.

   Das Fenster **Befehl senden** wird geöffnet.

3. Setzen Sie den Parameter **Funktion** auf **SMS-Clean** (s. Abb. unten).

4. Geben Sie im Feld **Telefonnummer** die Telefonnummer des Geräts ein, von dem Daten gelöscht werden sollen.

5. Geben Sie im Feld **Remote-Code** den Geheimcode des Geräts ein, an das die Nachricht gerichtet ist.

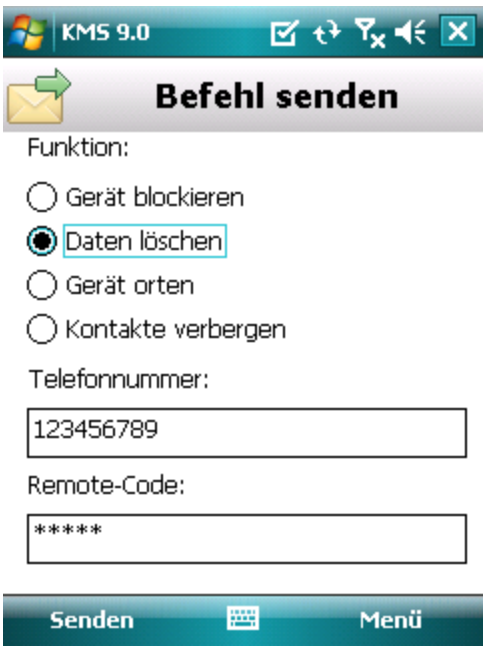


Abbildung 102. Löschen persönlicher Daten per Fernsteuerung starten

6. Klicken Sie auf **Senden**.

- *Um mit Hilfe der Standardfunktionen eines Handys eine SMS zu erstellen,*

  Schicken Sie an das vermisste / gestohlene Gerät eine SMS-Nachricht mit dem Text `wipe:<Code>` (wobei `<Code>` der Geheimcode des vermissten Geräts ist). Groß- und Kleinschreibung von Buchstaben sowie Leerzeichen vor und nach dem Doppelpunkt sind irrelevant.

LISTE DER ZU LÖSCHENDEN DATEN ERSTELLEN

Die Funktion SMS-Clean erlaubt es, eine Liste mit Ordnern anzulegen, die nach dem Empfang einer speziellen SMS-Nachricht gelöscht werden sollen.

- *Gehen Sie folgendermaßen vor, um einen Ordner zur Liste der zu löschenden Ordner hinzuzufügen:*

1. Gehen Sie auf **Menü** → **Diebstahlschutz**.

   Das Fenster **Diebstahlschutz** wird geöffnet.

2. Gehen Sie auf **SMS-Clean**.

   Das Fenster **SMS-Clean** wird geöffnet.

3. Gehen Sie auf **Zu löschende Ordner**.

   Das Fenster **Zu löschende Ordner** wird geöffnet.

4. Gehen Sie auf **Menü** → **Ordner hinzufügen** (s. Abb. unten).

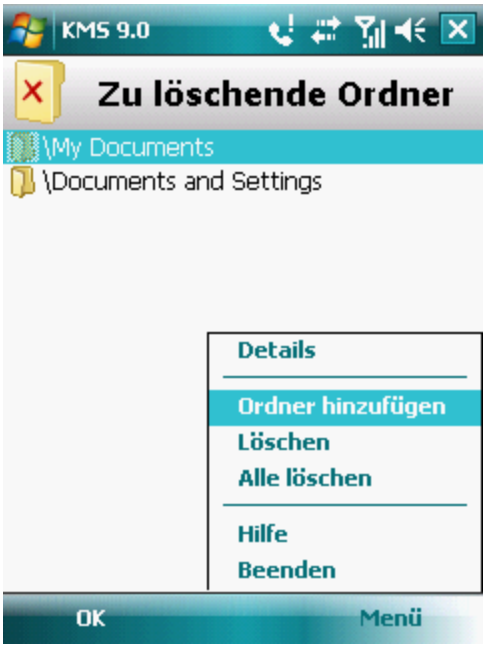


Abbildung 103. Zu löschende Ordner wählen

5. Wählen Sie den entsprechenden Ordner aus der Ordnerstruktur und klicken Sie auf **Auswählen**.

Der Ordner wird zur Liste hinzugefügt.

- *Gehen Sie folgendermaßen vor, um einen Ordner aus der Liste zu löschen (s. Abb. unten):*

1. Gehen Sie auf **Menü** → **Diebstahlschutz**.

Das Fenster **Diebstahlschutz** wird geöffnet.

2. Gehen Sie auf **SMS-Clean**.

   Das Fenster **SMS-Clean** wird geöffnet.

3. Gehen Sie auf **Zu löschende Ordner**.

   Das Fenster **Zu löschende Ordner** wird geöffnet.

4. Wählen Sie einen Ordner aus der Liste und gehen Sie auf **Menü → Löschen**.

WECHSEL DER SIM-KARTE AUF DEM GERÄT ÜBERWACHEN

Wenn die SIM-Karte auf dem verlorenen oder gestohlenen Gerät ausgetauscht wird, schickt SIM-Watch die neue Nummer der eingelegten SIM-Karte an eine vorgegebene Telefonnummer und / oder E-Mail-Adresse und blockiert das Gerät.

Gehen Sie folgendermaßen vor, um die Funktion SIM-Watch zu aktivieren und den Wechsel der SIM-Karte auf dem Gerät zu kontrollieren:

1. Gehen Sie auf **Menü → Diebstahlschutz**.

   Das Fenster **Diebstahlschutz** wird geöffnet.

2. Gehen Sie auf **SIM-Watch**.

   Das Fenster **SIM-Watch** wird geöffnet.

3. Aktivieren Sie das Kontrollkästchen **SIM-Watch aktivieren**.

4. Passen Sie folgende Parameter an, um den Wechsel der SIM-Karte auf dem Gerät zu kontrollieren (s. Abb. unten):

   - Um automatisch eine Nachricht über die neue Nummer Ihres Telefons zu erhalten, geben Sie unter **Neue Nummer senden** im Feld **Telefonnummer** die Nummer ein, die benachrichtigt werden soll.

     Die Nummer kann mit einer Ziffer oder dem Zeichen "+" beginnen und darf nur Ziffern enthalten.

   - Wenn Sie per E-Mail über die neue Nummer Ihres Telefons informiert werden möchten, geben Sie die entsprechende Adresse unter **Neue Nummer senden** im Feld **E-Mail-Adresse** ein.

   - Aktivieren Sie unter **Bei Wechsel der SIM-Karte** das Kontrollkästchen **Gerät blockieren**, damit das Gerät blockiert wird, wenn die SIM-Karte ausgetauscht oder das Gerät ohne SIM eingeschaltet wird. Das Gerät kann durch Eingabe des Geheimcodes entsperrt werden.

   - Damit auf dem Display des blockierten Geräts eine Nachricht angezeigt wird, füllen Sie das Feld **Text beim Blockieren** aus. In der Grundeinstellung wird für die Meldung ein Standardtext verwendet, dem Sie die Nummer des Besitzers hinzufügen können.

Abbildung 104. Einstellungen die Funktion SIM-Watch

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

GEOGRAFISCHE KOORDINATEN DES GERÄTS ERMITTELN

Die Funktion GPS-Find ermittelt die geografischen Koordinaten des Geräts und schickt sie mit einer SMS oder E-Mail an das anfragende Gerät oder an eine vorgegebene E-Mail-Adresse.

Diese Funktion eignet sich nur für Geräte mit integriertem GPS-Empfänger. Der GPS-Empfänger wird bei Bedarf automatisch aktiviert.

Eine Ortung ist nur möglich, wenn sich das Gerät im Empfangsbereich von Satelliten befindet. Besteht im Augenblick der Anfrage kein Satellitenempfang, dann wird in regelmäßigen Abständen versucht, eine Verbindung herzustellen.

Gehen Sie folgendermaßen vor, um GPS-Find zu aktivieren:

1. Gehen Sie auf **Menü** → **Diebstahlschutz**.

   Das Fenster **Diebstahlschutz** wird geöffnet.

2. Gehen Sie auf **GPS-Find**.

   Das Fenster **GPS-Find** wird geöffnet.

3. Aktivieren Sie das Kontrollkästchen **GPS-Find aktivieren**.

   In der Grundeinstellung sendet Kaspersky Mobile Security 9.0 die Koordinaten des Geräts mit einer Antwort-SMS.

4. Wenn die Koordinaten des Geräts per E-Mail gesendet werden sollen, geben Sie für den Parameter **Koordinaten senden** die entsprechende E-Mail-Adresse an (s. Abb. unten).

Abbildung 105. Einstellungen der Funktion GPS-Find

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Wenn GPS-Find aktiviert ist, können die Koordinaten des Geräts auf folgende Weise ermittelt werden:

- Mit der Funktion **Befehl senden**. Dafür ist ein anderes Gerät erforderlich, auf dem Kaspersky Mobile Security 9.0 installiert ist. Auf dem Zweitgerät wird mit Kaspersky Mobile Security 9.0 eine spezielle SMS-Nachricht erstellt und an das verlorene Gerät gesendet. Sie enthält die Telefonnummer des Geräts und seinen Geheimcode. Der Empfang einer speziellen SMS bleibt auf dem vermissten / gestohlenen Gerät unbemerkt.

- Mit den Standardfunktionen eines Handys, die zum Erstellen einer SMS-Nachricht dienen. Auf dem anderen Gerät wird eine SMS-Nachricht, die aus einem speziellen Text und dem Geheimcode des vermissten/gestohlenen Geräts besteht, erstellt und gesendet.

Um ein Gerät per Fernsteuerung zu orten, wird die sichere Methode mit der Funktion Befehl senden empfohlen. In diesem Fall werden Befehl und Geheimcode in verschlüsselter Form gesendet.

Gehen Sie folgendermaßen vor, um einen Befehl an das vermisste / gestohlene Gerät zu senden:

1. Gehen Sie auf **Menü** → **Erweitert**.

   Das Fenster **Erweitert** wird geöffnet.

2. Gehen Sie auf **Befehl senden**.

   Das Fenster **Befehl senden** wird geöffnet.

3. Wählen Sie für den Parameter **Funktion** den Wert **Gerät orten** (s. Abb. unten).

4. Geben Sie im Feld **Telefonnummer** die Nummer des Geräts ein, das geortet werden soll.

5. Geben Sie im Feld **Remote-Code** den Geheimcode des Geräts ein, an das die Nachricht gerichtet ist.

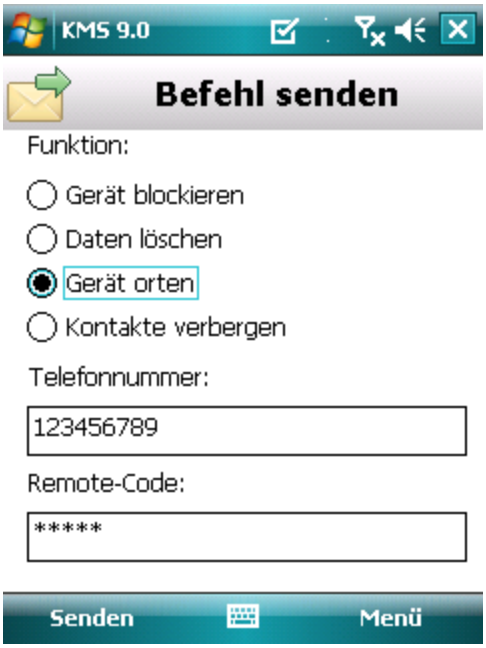


Abbildung 106. Gerät orten

6. Klicken Sie auf **Senden**.

- *Um mit Hilfe der Standardfunktionen eines Handys eine SMS zu erstellen,*

  schicken Sie an das vermisste / gestohlene Gerät eine SMS-Nachricht mit dem Text `find:<Code>` (wobei `<Code>` der Geheimcode des vermissten Geräts ist). Groß- und Kleinschreibung von Buchstaben sowie Leerzeichen vor und nach dem Doppelpunkt sind irrelevant.

Eine SMS-Nachricht mit den Koordinaten des Geräts wird gesendet an die Nummer, von der die Ortungsanfrage stammt, sowie an die E-Mail-Adresse, falls diese in den Einstellungen für GPS-Find angegeben wurde.

DIEBSTAHLSCHUTZ-FUNKTIONEN FERNGESTEUERT STARTEN

Mit einer speziellen SMS können Sie einen Befehl senden, um auf einem vermissten / gestohlenen Gerät, auf dem Kaspersky Mobile Security installiert ist, die Diebstahlschutz-Funktionen ferngesteuert zu starten. Der Empfang des Befehls bleibt auf dem zu blockierenden Gerät unbemerkt.

Es wird empfohlen, die Funktion **Befehl senden** zu verwenden, weil Befehl und Geheimcode dann in verschlüsselter Form an das vermisste / gestohlene Gerät übertragen werden.

- *Gehen Sie folgendermaßen vor, um einen Befehl an das vermisste / gestohlene Gerät zu senden:*

1. Gehen Sie auf **Menü** → **Erweitert**.

   Das Fenster **Erweitert** wird geöffnet.

2. Gehen Sie auf **Befehl senden**.

3. Das Fenster **Befehl senden** wird geöffnet.

4. Wählen Sie einen der folgenden Werte für **Funktion** (s. Abb. unten):

   - **SMS-Block**

- **SMS-Clean**
- **GPS-Find** (s. Abschnitt "Geografische Koordinaten des Geräts ermitteln" auf S. 168)
- **Privatsphäre** (s. Abschnitt "Persönliche Daten verbergen" auf S. 171)

5. Geben Sie im Feld **Telefonnummer** die Nummer des Geräts ein, an das die SMS geschickt wird.
6. Geben Sie im Feld **Remote-Code** den Geheimcode des Geräts ein, an das die Nachricht gerichtet ist.

Abbildung 107. Diebstahlschutz-Funktionen ferngesteuert starten

7. Klicken Sie auf **Senden**.

PERSÖNLICHE DATEN VERBERGEN

Dieser Abschnitt informiert über die Komponente *Privatsphäre*. Diese Komponente kann sensible Benutzerdaten schützen, wenn das Gerät vorübergehend von einer anderen Person verwendet wird.

IN DIESEM ABSCHNITT

Über die Privatsphäre 172

Über die Modi der Privatsphäre 172

Privatsphäre aktivieren / deaktivieren 172

Privatsphäre automatisch starten 173

Privatsphäre ferngesteuert starten 174

Liste der geschützten Kontakte erstellen 176

Schutzobjekte wählen: Privatsphäre 178

ÜBER DIE PRIVATSPHÄRE

Die Komponente *Privatsphäre* schützt persönliche Daten und verhindert unbefugten Zugriff auf sensible Informationen, wenn Ihr Gerät vorübergehend von anderen Personen verwendet wird. Die Komponente kann vertrauliche Benutzerdaten verbergen. Dazu zählen Kontakte (die im Gerätespeicher, auf der SIM-Karte oder auf einem Wechseldatenträger gespeichert sind), Nachrichten und Anrufe.

Die Komponente analysiert persönliche Daten auf Basis der Liste der geschützten Nummern (s. Abschnitt "Liste der geschützten Kontakte erstellen" auf S. 176). Für Nummern aus dieser Liste verbirgt die Komponente folgende Informationen:

- Informationen in der Kontaktliste
- Einträge über eine Nummer in der Anrufliste (Angenommen, Gewählt, Unbeantwortet)
- SMS-Nachrichten in der Liste der eingehenden, ausgehenden, gelöschten und gesendeten SMS-Nachrichten.

Informationen über die Arbeit der Privatsphäre werden in einem Bericht erfasst (s. Abschnitt "Programmberichte" auf S. 191).

ÜBER DIE MODI DER PRIVATSPHÄRE

Kaspersky Mobile Security 9.0 erlaubt es, den Schutz für persönliche Daten zu verwalten. Die Komponente *Privatsphäre* wird manuell gestartet. Sie ist standardmäßig deaktiviert.

Die Privatsphäre bietet folgende Modi:

- **Anzeigen** – Der Schutz für vertrauliche Daten ist deaktiviert. Die Einstellungen der Privatsphäre können geändert werden.
- **Verbergen** – Der Schutz für vertrauliche Daten ist aktiviert. Die Komponente Privatsphäre verbirgt alle Daten, die mit geschützten Kontakten zusammenhängen. Die Einstellungen der Privatsphäre können nicht geändert werden.

Der aktuelle Status der Komponente wird im Fenster **Privatsphäre** neben dem Menüpunkt **Modus** angezeigt.

Es kann eine gewisse Zeit beanspruchen, bis eine Modusänderung der Privatsphäre wirksam wird.

PRIVATSPHÄRE AKTIVIEREN / DEAKTIVIEREN

Der Privatsphären-Modus kann folgendermaßen geändert werden:

- aus dem Menü für die Einstellungen der Komponente
- aus dem Menü für **Privatsphäre**

Gehen Sie folgendermaßen vor, um den Privatsphären-Modus zu ändern:

1. Gehen Sie auf **Menü** → **Privatsphäre**.

   Das Fenster **Privatsphäre** wird geöffnet.

2. Gehen Sie auf **Modus**.

   Das Fenster **Modus** wird geöffnet.

3. Wählen Sie einen Wert für **Modus** (s. Abb. unten).

4. Klicken Sie auf **OK**.

Abbildung 108. Privatsphären-Modus ändern

5. Bestätigen Sie, dass der Privatsphären-Modus geändert werden soll. Klicken Sie dazu auf **Ja**.

Gehen Sie folgendermaßen vor, um den Privatsphären-Modus schnell zu ändern:

1. Gehen Sie auf **Menü** → **Privatsphäre**.

   Das Fenster **Privatsphäre** wird geöffnet.

2. Klicken Sie auf **Verbergen** / **Anzeigen**. Die Beschriftung der Schaltfläche ändert sich abhängig vom aktuellen Modus der Privatsphäre in das jeweilige Gegenteil.

3. Bestätigen Sie, dass der Privatsphären-Modus geändert werden soll. Klicken Sie dazu auf **Ja**.

PRIVATSPHÄRE AUTOMATISCH STARTEN

In der Grundeinstellung wird der Schutz für vertrauliche Daten sofort nach dem Einschalten der Privatsphäre gestartet.

Sie können eine Zeitspanne festlegen, nach deren Ablauf die Komponente *Privatsphäre* automatisch aktiviert werden soll.

Deaktivieren Sie die Privatsphäre, bevor die Einstellungen geändert werden sollen.

Gehen Sie folgendermaßen vor, um festzulegen, dass die Privatsphäre nach Ablauf eines bestimmten Zeitraums automatisch gestartet werden soll:

1. Gehen Sie auf **Menü** → **Privatsphäre**.

   Das Fenster **Privatsphäre** wird geöffnet.

2. Gehen Sie auf **Modus**.

3. Das Fenster **Modus** wird geöffnet.

4. Aktivieren Sie das Kontrollkästchen **Zugriff verbieten** (s. Abb. unten).

5. Legen Sie einen Zeitraum fest, nach dem die Komponente Privatsphäre automatisch gestartet werden soll. Wählen Sie dazu einen der folgenden Werte für **Timeout**:

   - **Sofort**
   - **In 1 Minute**
   - **In 5 Minuten**
   - **In 15 Minuten**
   - **In 1 Stunde**

Abbildung 109. Einstellungen für den automatischen Start der Privatsphäre

6. Klicken Sie auf **OK**.

PRIVATSPHÄRE FERNGESTEUERT STARTEN

Kaspersky Mobile Security 9.0 erlaubt es, die Privatsphäre mit einer speziellen SMS ferngesteuert zu starten. Dazu muss vorher die Funktion aktiviert werden, die den Remote-Start der Privatsphäre erlaubt.

➡ *Gehen Sie folgendermaßen vor, um den ferngesteuerten Start der Privatsphäre zu erlauben:*

1. Gehen Sie auf **Menü** → **Privatsphäre**.

   Das Fenster **Privatsphäre** wird geöffnet.

2. Gehen Sie auf **Modus**.

   Das Fenster **Modus** wird geöffnet.

3. Aktivieren Sie das Kontrollkästchen **Bei SMS verbergen** (s. Abb. unten).

Abbildung 110. Einstellungen für das ferngesteuerte Aktivieren der Privatsphäre

4. Klicken Sie auf **OK**.

Für den ferngesteuerten Start der Komponente *Privatsphäre* bestehen folgende Möglichkeiten:

- Befehl an das vermisste / gestohlene Gerät senden. Dafür ist ein anderes Gerät erforderlich, auf dem Kaspersky Mobile Security 9.0 installiert ist. Auf dem Zweitgerät wird mit Kaspersky Mobile Security 9.0 eine spezielle SMS-Nachricht erstellt und an das verlorene Gerät gesendet. Sie enthält die Telefonnummer des Geräts und seinen Geheimcode. Der Empfang einer speziellen SMS bleibt auf dem vermissten / gestohlenen Gerät unbemerkt.

- Mit den Standardfunktionen des Telefons, die zum Erstellen einer SMS-Nachricht dienen. Auf dem anderen Gerät wird eine SMS-Nachricht, die aus einem speziellen Text und dem Geheimcode des vermissten/gestohlenen Geräts besteht, erstellt und gesendet.

Gehen Sie folgendermaßen vor, um einen Befehl an das vermisste / gestohlene Gerät zu senden:

1. Gehen Sie auf **Menü** → **Erweitert**.

   Das Fenster **Erweitert** wird geöffnet.

2. Gehen Sie auf **Befehl senden**.

   Das Fenster **Befehl senden** wird geöffnet.

3. Wählen Sie für den Parameter **Funktion** den Wert **Kontakte verbergen** (s. Abb. unten).

4. Geben Sie im Feld **Telefonnummer** die Nummer des Geräts ein, das geortet werden soll.

5. Geben Sie im Feld **Remote-Code** den Geheimcode des Geräts ein, an das die Nachricht gerichtet ist.

Abbildung 111. Privatsphäre ferngesteuert starten

6. Klicken Sie auf **Senden**.

Nach dem Empfang des Befehls wird die Komponente Privatsphäre automatisch auf dem verlorenen / gestohlenen Gerät gestartet.

Um mit Hilfe der Standardfunktionen eines Telefons eine SMS zu erstellen:

Schicken Sie an das zu blockierende Gerät eine SMS-Nachricht mit dem Text `hide:<Code>` (wobei `<Code>` der Geheimcode des vermissten Geräts ist). Die Groß- und Kleinschreibung von Buchstaben und die Leerzeichen vor und nach dem Doppelpunkt sind irrelevant.

LISTE DER GESCHÜTZTEN KONTAKTE ERSTELLEN

Die Komponente *Privatsphäre* verbirgt persönliche Daten (z.B. SMS-Nachrichten und Anrufe), die mit bestimmten Kontakten zusammenhängen. Solche Telefonnummern werden in der Liste der geschützten Kontakte gespeichert.

IN DIESEM ABSCHNITT

Nummer zur Liste der geschützten Kontakte hinzufügen 176

Nummer in der Liste der geschützten Kontakte ändern 177

Nummer aus der Liste der geschützten Kontakte löschen 178

NUMMER ZUR LISTE DER GESCHÜTZTEN KONTAKTE HINZUFÜGEN

Deaktivieren Sie die Privatsphäre, bevor die Einstellungen geändert werden sollen.

Gehen Sie folgendermaßen vor, um der Liste der geschützten Kontakte eine Telefonnummer hinzuzufügen:

1. Gehen Sie auf **Menü** → **Privatsphäre**.

Das Fenster **Privatsphäre** wird geöffnet.

2. Gehen Sie auf **Kontaktliste**.

   Das Fenster **Kontaktliste** wird geöffnet.

3. Führen Sie im nächsten Fenster eine der folgenden Aktionen aus (s. Abb. unten):

   - Um eine Nummer aus dem Telefonbuch hinzuzufügen, gehen Sie auf **Menü** → **Hinzufügen** → **Outlook-Kontakt**. Wählen Sie im folgenden Fenster **Outlook-Kontakte** den entsprechenden Eintrag und klicken Sie dann auf **Auswählen**.

   - Gehen Sie auf **Menü** → **Hinzufügen** → **Kontakt von SIM**, um eine Nummer hinzuzufügen, die auf der SIM-Karte gespeichert ist. Wählen Sie im folgenden Fenster **Kontakt von SIM** den entsprechenden Eintrag und klicken Sie dann auf **OK**.

   - Um eine Nummer manuell hinzuzufügen, gehen Sie auf **Menü** → **Hinzufügen** → **Nummer**. Füllen Sie im folgenden Fenster **Eintrag hinzufügen** das Feld **Telefonnummer** aus und klicken Sie auf **OK**.

Abbildung 112. Nummer zur Liste der geschützten Kontakte hinzufügen

Die Telefonnummer wird zur Liste der geschützten Kontakte hinzugefügt.

NUMMER IN DER LISTE DER GESCHÜTZTEN KONTAKTE ÄNDERN

Deaktivieren Sie die Privatsphäre, bevor die Einstellungen geändert werden sollen.

Es können nur Nummern geändert werden, die im Programm selbst eingegeben wurden. Nummern, die aus der Kontaktliste oder aus der SIM-Nummernliste hinzugefügt wurden, können nicht geändert werden.

➡ *Gehen Sie folgendermaßen vor, um eine Nummer in der Liste der geschützten Kontakte zu ändern:*

1. Gehen Sie auf **Menü** → **Privatsphäre**.

   Das Fenster **Privatsphäre** wird geöffnet.

2. Gehen Sie auf **Kontaktliste**.

Das Fenster **Kontaktliste** wird geöffnet.

3. Wählen Sie eine Nummer, die geändert werden soll, und gehen Sie dann auf **Menü → Nummer ändern**.

   Das Fenster **Einträg ändern** wird geöffnet.

4. Ändern Sie die Daten im Feld **Telefonnummer**.

5. Klicken Sie nach Abschluss der Änderungen auf **OK**.

Die Nummer wird geändert.

NUMMER AUS DER LISTE DER GESCHÜTZTEN KONTAKTE LÖSCHEN

Sie können eine Nummer löschen oder die gesamte Liste der geschützten Kontakte leeren.

Deaktivieren Sie die Privatsphäre, bevor die Einstellungen geändert werden sollen.

- *Gehen Sie folgendermaßen vor, um eine Nummer aus der Liste der geschützten Kontakte zu löschen:*

  1. Gehen Sie auf **Menü → Privatsphäre**.

     Das Fenster **Privatsphäre** wird geöffnet.

  2. Gehen Sie auf **Kontaktliste**.

  3. Das Fenster **Kontaktliste** wird geöffnet.

  4. Wählen Sie eine Nummer, die gelöscht werden soll, und gehen Sie dann auf **Menü → Eintrag löschen**.

  5. Bestätigen Sie das Löschen. Klicken Sie dazu auf **Ja**.

- *Gehen Sie folgendermaßen vor, um die Liste der geschützten Kontakte zu leeren:*

  1. Gehen Sie auf **Menü → Privatsphäre**.

     Das Fenster **Privatsphäre** wird geöffnet.

  2. Gehen Sie auf **Kontaktliste**.

  3. Das Fenster **Kontaktliste** wird geöffnet.

  4. Gehen Sie auf **Menü → Alle löschen**.

  5. Bestätigen Sie das Löschen. Klicken Sie dazu auf **Ja**.

Die Liste der geschützten Kontakte wird geleert.

SCHUTZOBJEKTE WÄHLEN: PRIVATSPHÄRE

Wenn die Komponente *Privatsphäre* aktiviert ist, werden standardmäßig Kontakte, Nachrichten und Einträge in der Anrufliste verborgen, die mit geschützten Kontakten zusammenhängen. Sie können die Daten wählen, auf die der Zugriff verboten werden soll.

Deaktivieren Sie die Privatsphäre, bevor die Einstellungen geändert werden sollen.

Gehen Sie folgendermaßen vor, um Schutzobjekte zu wählen:

1. Gehen Sie auf **Menü** → **Privatsphäre**.

   Das Fenster **Privatsphäre** wird geöffnet.

2. Gehen Sie auf **Verborgene Objekte**.

   Das Fenster **Verborgene Objekte** wird geöffnet (s. Abb. unten).

3. Wählen Sie im Block **Einträge verbergen**, welche auf dem Gerät gespeicherten Daten verborgen werden sollen. Folgende Varianten stehen zur Auswahl:

   - **Kontakte** – Im Telefonbuch werden alle Daten über geschützte Nummern verborgen.
   - **SMS** – In der Liste der eingehenden / ausgehenden SMS-Nachrichten werden alle SMS von geschützten Nummern verborgen.
   - **Anrufe** – Anrufe von geschützten Nummern können angenommen werden. Die Nummer des Anrufers wird aber ausgeblendet und Infos über geschützte Nummern in der Anrufliste (Angenommen, Gewählt, Unbeantwortet) werden verborgen.

4. Wählen Sie im Block **Ereignisse verbergen**, welcher Typ der eingehenden Daten verborgen werden soll. Folgende Ereignisse können verborgen werden:

   - **Eingehende SMS** – Der Empfang eingehender SMS-Nachrichten wird nicht angezeigt (auf dem Display erscheint kein Hinweis darüber, dass eine neue SMS-Nachricht von einer verborgenen Nummer empfangen wurde). Alle SMS-Nachrichten, die von geschützten Nummern empfangen wurden, können gelesen werden, wenn die Privatsphäre deaktiviert wurde.
   - **Eingehende Anrufe** – Anrufe von geschützten Nummern werden blockiert (Der Anrufer hört ein "Besetzt"-Zeichen). Nachdem die Privatsphäre deaktiviert wurde, können Informationen über den unbeantworteten Anruf angezeigt werden.

Abbildung 113. Verborgene Objekte wählen

5. Klicken Sie auf **OK**.

NETZWERKAKTIVITÄT FILTERN

Dieser Abschnitt informiert über die Komponente *Firewall*, die ein- und ausgehende Verbindungen auf Ihrem Gerät kontrolliert. Außerdem wird hier beschrieben, wie die Komponente aktiviert / deaktiviert wird und wie die gewünschte Sicherheitsstufe gewählt wird.

IN DIESEM ABSCHNITT

Firewall.....180

Firewall aktivieren / deaktivieren.....180

Sicherheitsstufe der Firewall wählen.....180

FIREWALL

Die Firewall analysiert alle Netzwerkverbindungen auf Ihrem Gerät. In Abhängigkeit der gewählten Sicherheitsstufe blockiert oder erlaubt sie bestimmte Netzwerkaktivitäten.

Die Firewall ist nach der Installation von Kaspersky Mobile Security 9.0 standardmäßig deaktiviert.

Informationen über die Arbeit der Firewall werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. 191).

FIREWALL AKTIVIEREN / DEAKTIVIEREN

Die Arbeit der Firewall ist von der ausgewählten Sicherheitsstufe abhängig. Die jeweils geltende Sicherheitsstufe definiert, über welche Netzwerkprotokolle die Datenübertragung zugelassen und über welche sie gesperrt wird.

Es sind folgende Sicherheitsstufen vorgesehen:

- **Aus** – jede Netzwerkaktivität erlauben. Diese Sicherheitsstufe ist standardmäßig altiviert.
- **Minimaler Schutz** – nur eingehende Verbindungen blockieren. Ausgehende Verbindungen werden erlaubt.
- **Maximaler Schutz** – alle eingehenden Verbindungen blockieren. Prüfen eines E-Mail-Postfachs, Anzeige von Webseiten und Download von Dateien sind erlaubt. Ausgehende Verbindungen können nur über die Ports SSH, HTTP, HTTPS, IMAP, SMTP, POP3 erfolgen.
- **Alle blockieren** – jede Netzwerkaktivität außer Datenbank-Update und Lizenzverlängerung blockieren.

Sie können die Sicherheitsstufe der Firewall ändern (s. Abschnitt "Sicherheitsstufe der Firewall wählen" auf S. 180). Der aktuelle Modus wird im Fenster **Firewall** neben dem Menüpunkt **Modus** angezeigt.

SICHERHEITSSTUFE DER FIREWALL WÄHLEN

Verwenden Sie den Joystick oder die Navigationstasten des Geräts, um die Parameterwerte zu ändern.

Gehen Sie folgendermaßen vor, um eine Sicherheitsstufe für die Firewall zu wählen:

1. Gehen Sie auf **Menü** → **Firewall**.

   Das Fenster **Firewall** wird geöffnet.

2. Gehen Sie auf **Modus**.

   Das Fenster **Einstellungen** wird geöffnet.

3. Wählen Sie eine Sicherheitsstufe (s. Abb. unten).

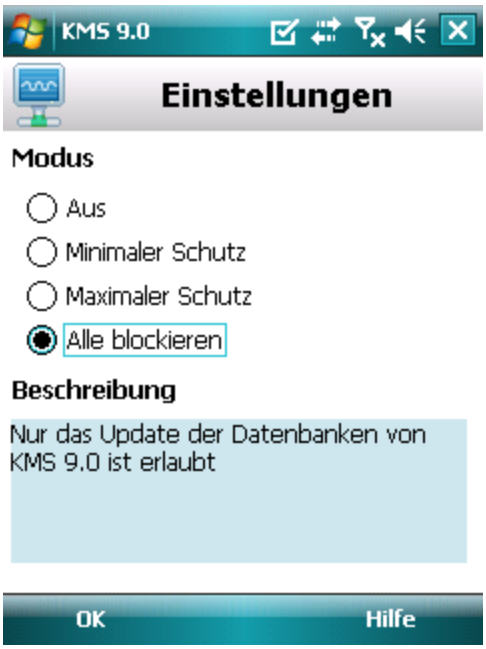


Abbildung 114. Sicherheitsstufe der Firewall wählen

4. Klicken Sie auf **OK**.

PERSÖNLICHE DATEN VERSCHLÜSSELN

Dieser Abschnitt informiert über die Komponente *Verschlüsselung*, die sensible Daten auf Ihrem Gerät schützt. Außerdem wird hier beschrieben, wie die Komponente aktiviert / deaktiviert wird und wie ausgewählte Ordner verschlüsselt / entschlüsselt werden können.

IN DIESEM ABSCHNITT

Verschlüsselung 181

Daten verschlüsseln 182

Daten entschlüsseln 183

Zugriff auf verschlüsselte Daten verbieten 185

VERSCHLÜSSELUNG

Die Komponente *Verschlüsselung* schützt die Daten auf dem Gerät auch dann vor dem Zugriff durch Dritte, wenn das Gerät in fremde Hände geraten sollte. Die Komponente erlaubt es, eine beliebige Anzahl von Ordnern, die nicht zum System gehören, zu verschlüsseln.

Um Daten zu verschlüsseln / entschlüsseln, geben Sie den Geheimcode ein (s. Abschnitt "Geheimcode eingeben" auf S. 117). Wenn das Gerät in den Stromsparmodus gewechselt hat und die festgelegte Zeitspanne abgelaufen ist (s. Abschnitt "Zugriff auf verschlüsselte Daten verbieten" auf S. 185), wird der Datenzugriff automatisch blockiert.

Die Daten in einem Ordner werden durch den Befehl **Verschlüsseln** chiffriert. Künftig werden die Daten automatisch ver- und entschlüsselt, wenn Daten in dem Ordner gespeichert oder daraus gelesen werden oder wenn auf die Daten zugegriffen wird.

Der Start von EXE-Dateien aus einem verschlüsselten Ordner wird nicht unterstützt.

Die Komponente *Verschlüsselung* ist nach der Installation von Kaspersky Mobile Security 9.0 standardmäßig deaktiviert.

Informationen über die Arbeit der Komponente werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. 191).

DATEN VERSCHLÜSSELN

Die Komponente *Verschlüsselung* erlaubt es, eine beliebige Anzahl von Ordnern, die nicht zum System gehören, zu verschlüsseln. Die Ordner können sich im Speicher des Geräts oder auf einer Speicherkarte befinden.

Eine Liste aller bisher verschlüsselten und entschlüsselten Ordner befindet sich im Fenster **Verschlüsselung** unter dem Menüpunkt **Ordnerliste**.

Es ist auch möglich, alle Ordner, die in der Ordnerliste stehen, gleichzeitig zu verschlüsseln.

Gehen Sie folgendermaßen vor, um Daten zu verschlüsseln:

1. Gehen Sie auf **Menü** → **Verschlüsselung**.

   Das Fenster **Verschlüsselung** wird geöffnet.

2. Gehen Sie auf **Ordnerliste**.

   Das Fenster **Ordnerliste** wird geöffnet.

3. Klicken Sie auf **Menü** → **Ordner hinzufügen**.

   Ein Fenster mit einer Übersicht des Dateisystems Ihres Geräts wird geöffnet.

4. Wählen Sie den Ordner, der verschlüsselt werden soll, und klicken Sie dann auf **Verschlüsseln** (s. Abb. unten).

Verwenden Sie zur Navigation im Dateisystem den Joystick oder die Navigationstasten des Geräts.

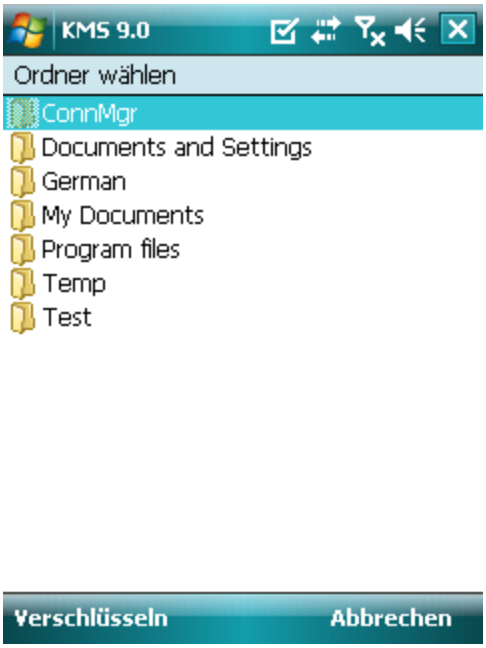


Abbildung 115. Daten verschlüsseln

Sie werden von Kaspersky Mobile Security 9.0 benachrichtigt, wenn der Verschlüsselungsvorgang abgeschlossen wurde. Es erscheint ein Meldungsfenster.

5. Klicken Sie auf **OK**.

   Für einen verschlüsselten Ordner ändert sich im **Menü** der Punkt **Verschlüsseln** in **Entschlüsseln**.

Nach der Verschlüsselung werden Daten automatisch ent- und verschlüsselt, wenn Sie mit den Daten in einem verschlüsselten Ordner arbeiten, Daten aus einem verschlüsselten Ordner entnehmen oder neue Daten darin speichern.

Gehen Sie folgendermaßen vor, um alle Ordner der Liste auf einmal zu verschlüsseln:

1. Gehen Sie auf **Menü** → **Verschlüsselung**.

   Das Fenster **Verschlüsselung** wird geöffnet.

2. Gehen Sie auf **Ordnerliste**.

   Das Fenster **Ordnerliste** wird geöffnet.

3. Gehen Sie auf **Menü** → **Zusatzaktionen** → **Alle verschlüsseln**.

   Sie werden von Kaspersky Mobile Security 9.0 benachrichtigt, wenn der Verschlüsselungsvorgang abgeschlossen wurde. Es erscheint ein Meldungsfenster.

4. Klicken Sie auf **OK**.

DATEN ENTSCHLÜSSELN

Sie können zuvor verschlüsselte Daten vollständig entschlüsseln (s. Abschnitt "Datenverschlüsselung" auf S. 182). Sie können einen oder alle verschlüsselten Ordner auf dem Gerät entschlüsseln.

Gehen Sie folgendermaßen vor, um einen zuvor verschlüsselten Ordner zu entschlüsseln:

1. Gehen Sie auf **Menü** → **Verschlüsselung**.

   Das Fenster **Verschlüsselung** wird geöffnet.

2. Gehen Sie auf **Ordnerliste**.

   Das Fenster **Ordnerliste** wird geöffnet. Es enthält eine Liste aller bisher ver- und entschlüsselten Ordner.

3. Wählen Sie einen verschlüsselten Ordner aus der Liste und klicken Sie auf **Menü** → **Entschlüsseln** (s. Abb. unten).

Abbildung 116. Funktion aktivieren

   Sie werden von Kaspersky Mobile Security 9.0 benachrichtigt, wenn der Entschlüsselungsvorgang abgeschlossen wurde. Es erscheint ein Meldungsfenster.

4. Klicken Sie auf **OK**.

Für einen verschlüsselten Ordner ändert sich im **Menü** der Punkt **Entschlüsseln** in **Verschlüsseln**. Sie können die Datenverschlüsselung erneut verwenden (s. Abschnitt "Daten verschlüsseln" auf S. 182).

Gehen Sie folgendermaßen vor, um alle Ordner der Liste auf einmal zu entschlüsseln:

1. Gehen Sie auf **Menü** → **Firewall**.

   Das Fenster **Firewall** wird geöffnet.

2. Gehen Sie auf **Ordnerliste**.

   Das Fenster **Ordnerliste** wird geöffnet.

3. Gehen Sie auf **Menü** → **Zusatzaktionen** → **Alle entschlüsseln**.

   Sie werden von Kaspersky Mobile Security 9.0 benachrichtigt, wenn der Entschlüsselungsvorgang abgeschlossen wurde. Es erscheint ein Meldungsfenster.

4. Klicken Sie auf **OK**.

ZUGRIFF AUF VERSCHLÜSSELTE DATEN VERBIETEN

Die Komponente *Verschlüsselung* kann den Zugriff auf verschlüsselte Daten entweder sofort blockieren oder nach Ablauf einer festgelegten Zeitspanne ab dem Wechsel des Geräts in den Stromsparmodus.

Standardmäßig wird der Zugriff auf verschlüsselte Daten sofort blockiert, nachdem sich die Hintergrundbeleuchtung des Bildschirms ausschaltet.

Sie können festlegen, nach welchem Zeitraum verschlüsselte Daten blockiert werden sollen, wenn das Gerät in den Stromsparmodus wechselt. Um danach mit verschlüsselten Daten zu arbeiten, muss der Geheimcode eingegeben werden (s. Abschnitt "Geheimcode eingeben" auf S. 117).

Außerdem können Sie den Zugriff auf verschlüsselte Daten sofort verbieten und die Abfrage des Geheimcodes aktivieren.

Gehen Sie folgendermaßen vor, um den Zugriff auf einen Zugriff zeitverzögert zu verbieten:

1. Gehen Sie auf **Menü** → **Verschlüsselung**.

   Das Fenster **Verschlüsselung** wird geöffnet.

2. Gehen Sie auf **Zugriff verbieten**.

   Das Fenster **Zugriff verbieten** wird geöffnet.

3. Legen Sie fest, wie lange die Daten noch verfügbar sein sollen, nachdem das Gerät in den Stromsparmodus gewechselt hat. Wählen Sie dazu für **Zugriff verbieten** einen der folgenden Werte (s. Abb. unten):

   - **Sofort**
   - **In 1 Minute**
   - **In 5 Minuten**
   - **In 15 Minuten**
   - **In 1 Stunde**

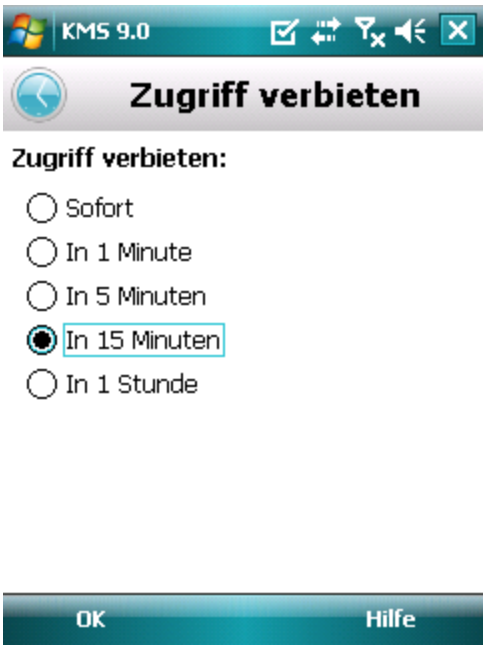


Abbildung 117. Zugriff auf verschlüsselte Daten blockieren

4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Um den Zugriff auf einen Ordner sofort zu blockieren,

klicken Sie in der Taskleiste des Geräts auf das Symbol von Kaspersky Mobile Security 9.0 und den Punkt **Daten blockieren** (s. Abb. unten).

Abbildung 118. Kontextmenü des Programms in der Taskleiste des Geräts

UPDATE DER PROGRAMM-DATENBANKEN

Dieser Abschnitt informiert über das Update der Programm-Datenbanken. Das Update hält den Schutz Ihres Geräts auf dem neusten Stand. Außerdem werden hier folgende Vorgänge beschrieben: Informationen über die installierten Programm-Datenbanken anzeigen, Updatevorgang manuell starten, automatisches Datenbank-Update anpassen.

IN DIESEM ABSCHNITT

Über das Update der Programm-Datenbanken....186

Datenbankinfos anzeigen....187

Manuelles Update....188

Update nach Zeitplan....189

Update im Roaming....190

ÜBER DAS UPDATE DER PROGRAMM-DATENBANKEN

Die Suche erfolgt auf Basis von Programm-Datenbanken, die eine Beschreibung aller momentan bekannten schädlichen Programme und entsprechende Desinfektionsmethoden sowie eine Beschreibung sonstiger unerwünschter Objekte enthalten. Es ist sehr wichtig, die Datenbanken auf dem neuesten Stand zu halten.

Es wird empfohlen, die Programm-Datenbanken regelmäßig zu aktualisieren. Die Daten gelten als stark veraltet, wenn seit dem letzten Update 15 Tage vergangen sind. In diesem Fall kann die Zuverlässigkeit des Schutzes nicht mehr garantiert werden.

Kaspersky Mobile Security 9.0 lädt seine Updates von Kaspersky-Lab-Updateservern herunter. Dabei handelt es sich um spezielle Internetseiten, auf denen Updates der Datenbanken für alle Kaspersky-Lab-Produkte zur Verfügung gestellt werden.

Um die Programm-Datenbanken zu aktualisieren, muss auf dem mobilen Gerät eine Internetverbindung eingerichtet sein.

Die Aktualisierung der Programm-Datenbanken wird nach folgendem Ablauf ausgeführt:

1. Die Programm-Datenbanken auf Ihrem mobilen Gerät werden mit den Datenbanken verglichen, die sich auf dem Kaspersky-Lab-Updateserver befinden.

2. Kaspersky Mobile Security 9.0 führt eine der folgenden Aktionen aus:

   - Wenn Ihre Programm-Datenbanken aktuell sind, wird eine entsprechende Meldung angezeigt.

   - Wenn sich die installierten Datenbanken von den angebotenen unterscheiden, wird ein neues Updatepaket heruntergeladen und installiert.

     Die Verbindung wird nach Abschluss des Updatevorgangs automatisch getrennt. Eine Verbindung, die bereits vor dem Update aufgebaut wurde, bleibt bestehen.

Sie können die Updateaufgabe entweder manuell starten, wenn das Gerät nicht für andere Aufgaben benötigt wird, oder einen Zeitplan für das automatische Update einstellen.

Ausführliche Informationen über die verwendeten Datenbanken stehen im Fenster **Erweitert** unter dem Menüpunkt **Datenbank-Infos** zur Verfügung.

Informationen über das Datenbank-Update werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. 191).

DATENBANK-INFOS ANZEIGEN

Sie können Informationen über die installierten Programm-Datenbanken anzeigen. Folgende Daten sind verfügbar: Datum des letzten Updates, Erscheinungsdatum der Datenbanken und Anzahl der Einträge in den Datenbanken.

Gehen Sie folgendermaßen vor, um Informationen über die installierten Datenbanken anzuzeigen:

1. Gehen Sie auf **Menü** → **Erweitert**.

   Das Fenster **Erweitert** wird geöffnet.

2. Wählen Sie **Datenbank-Infos**.

Das folgende Fenster **Datenbank-Infos** informiert über die installierten Programm-Datenbanken (s. Abb. unten).

Abbildung 119. Informationen über die installierten Programm-Datenbanken

MANUELLES UPDATE

Sie können das Update der Programm-Datenbanken manuell starten.

Gehen Sie folgendermaßen vor, um das Update der Programm-Datenbanken zu starten:

1. Gehen Sie auf **Menü** → **Anti-Virus**.

   Das Fenster **Anti-Virus** wird geöffnet.

2. Gehen Sie auf **Update**.

   Das Fenster **Update** wird geöffnet.

3. Gehen Sie auf **Update** (s. Abb. unten).

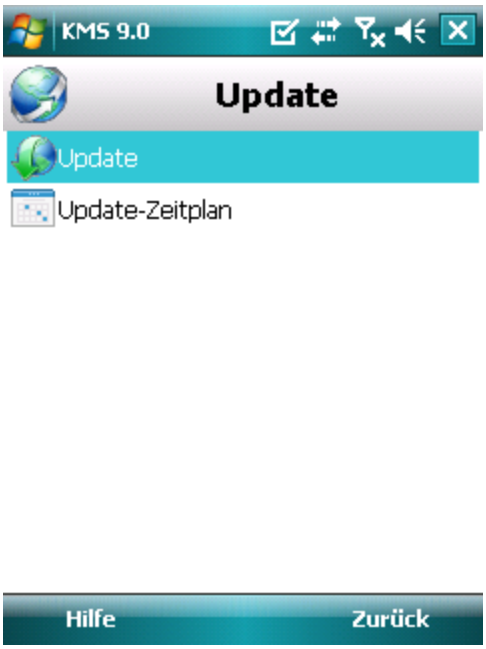


Abbildung 120. Update manuell starten

Das Programm startet das Update der Datenbanken von einem Kaspersky-Lab-Server. Informationen über den Updatevorgang werden auf dem Bildschirm angezeigt.

UPDATE NACH ZEITPLAN

Eine wichtige Voraussetzung für die Sicherheit des Geräts besteht darin, den Schutz auf dem neusten Stand zu halten. Sie können das automatische Update der Datenbanken festlegen.

➧ *Um einen Zeitplan einzurichten, nach dem die Datenbanken automatisch aktualisiert werden:*

1. Gehen Sie auf **Menü** → **Anti-Virus**.

   Das Fenster **Anti-Virus** wird geöffnet.

2. Gehen Sie auf **Update**.

   Das Fenster **Update** wird geöffnet.

3. Gehen Sie auf den Punkt **Update-Zeitplan**.

   Das Fenster **Zeitplan** wird geöffnet.

4. Aktivieren Sie das Kontrollkästchen **Update nach Zeitplan** (s. Abb. unten).

5. Erstellen Sie einen Zeitplan für das Update. Wählen Sie dazu einen Wert für den Parameter **Frequenz**:

   - **Täglich**: Die Programm-Datenbanken werden jeden Tag aktualisiert. Legen Sie dann einen Wert für **Zeit** fest.

   - **Wöchentlich**: Die Programm-Datenbanken werden ein Mal in der Woche aktualisiert. Legen Sie dann Werte für **Zeit** und **Wochentag** fest.

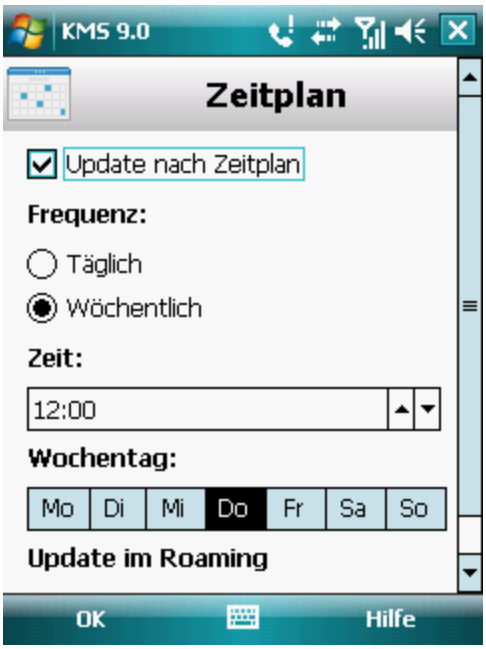


Abbildung 121. Einstellungen für automatisches Update

6. Klicken Sie auf **OK**, um die Änderungen zu speichern.

UPDATE IM ROAMING

Sie können festlegen, dass das geplante Update der Programm-Datenbanken im Roaming erlaubt / verboten wird. Falls im Roaming ein geplantes Update verboten wird, ist eine manuelle Aktualisierung im gewöhnlichen Modus möglich.

Gehen Sie folgendermaßen vor, um das geplante Update im Roaming zu erlauben:

1. Gehen Sie auf **Menü** → **Anti-Virus**.

   Das Fenster **Anti-Virus** wird geöffnet.

2. Gehen Sie auf **Update**.

   Das Fenster **Update** wird geöffnet.

3. Gehen Sie auf den Punkt **Update-Zeitplan**.

   Das Fenster **Zeitplan** wird geöffnet.

4. Aktivieren Sie im Block **Update im Roaming** das Kontrollkästchen **Update im Roaming**.

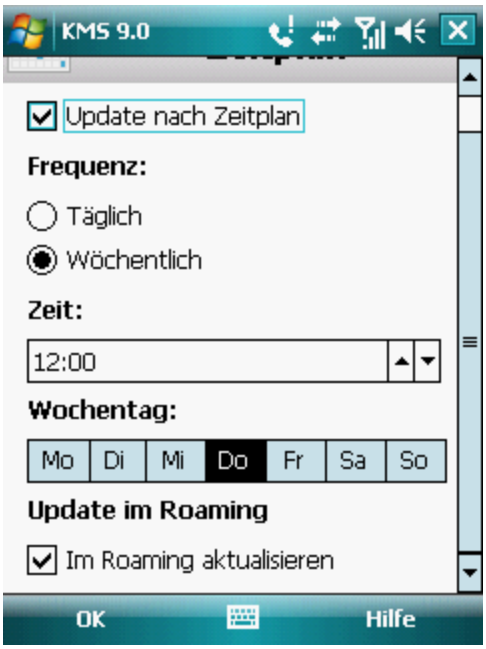


Abbildung 122. Update im Roaming anpassen

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

PROGRAMMBERICHTE

Dieser Abschnitt informiert über die Berichte, in denen die Arbeit der einzelnen Komponenten und die Ausführung aller Aufgaben (z.B. Update der Programm-Datenbanken, Virensuche, usw.) protokolliert werden.

IN DIESEM ABSCHNITT

Berichte....191

Berichtseinträge anzeigen....191

Einträge aus Bericht löschen....192

BERICHTE

In Berichten werden Ereignisse gespeichert, die bei der Arbeit der einzelnen Komponenten von Kaspersky Mobile Security 9.0 auftreten. Die Einträge sind in absteigender Reihenfolge nach dem Zeitpunkt der Ereignisse angeordnet.

Für jede Komponente wird ein eigener Ereignisbericht geführt.

BERICHTSEINTRÄGE ANZEIGEN

Gehen Sie folgendermaßen vor, um alle Einträge anzuzeigen:

1. Gehen Sie auf **Menü** → **Erweitert**.

   Das Fenster **Erweitert** wird geöffnet.

2. Wählen Sie den Punkt **Berichte**.

Das Fenster **Berichte** wird geöffnet.

3. Wählen Sie die Komponente, für die ein Ereignisbericht angezeigt werden soll.

Der Ereignisbericht der gewählten Komponente wird geöffnet (s. Abb. unten).

Abbildung 123. Berichtseinträge anzeigen

- *Um ausführliche Informationen über einen Berichtseintrag anzuzeigen,*

  wählen Sie einen Eintrag und klicken Sie auf **Details**.

- *Um zur Berichtsliste zurückzukehren,*

  klicken Sie auf **Menü → Zurück**.

EINTRÄGE AUS BERICHT LÖSCHEN

Sie können alle Berichte leeren. Die Informationen über die Arbeit aller Komponenten von Kaspersky Mobile Security 9.0 werden gelöscht.

- *Gehen Sie folgendermaßen vor, um alle Berichte zu leeren:*

  1. Gehen Sie auf **Menü → Erweitert**.

     Das Fenster **Erweitert** wird geöffnet.

  2. Wählen Sie den Punkt **Berichte**.

     Das Fenster **Berichte** wird geöffnet.

  3. Öffnen Sie den Bericht einer beliebigen Komponente.

4. Gehen Sie auf **Menü** → **Alle löschen** (s. Abb. unten).

Abbildung 124. Einträge löschen

5. Bestätigen Sie die Deinstallation mit **Ja**.

Es werden alle Einträge im Bericht aller Komponenten gelöscht.

ERWEITERTE EINSTELLUNGEN ANPASSEN

Dieser Abschnitt informiert über zusätzliche Optionen von Kaspersky Mobile Security 9.0: Geheimcode ändern, Audiosignale des Programms verwalten, Anzeige von Tooltips aktivieren / deaktivieren.

IN DIESEM ABSCHNITT

Geheimcode ändern 193

Tooltips anzeigen 194

Audiosignale verwalten 195

GEHEIMCODE ÄNDERN

Der Geheimcode, der nach der Programmaktivierung festgelegt wurde, kann geändert werden.

Gehen Sie folgendermaßen vor, um den Geheimcode zu ändern:

1. Gehen Sie auf **Menü** → **Erweitert**.

   Das Fenster **Erweitert** wird geöffnet.

2. Gehen Sie auf **Einstellungen**.

   Das Fenster **Einstellungen** wird geöffnet.

3. Gehen Sie auf **Code ändern**.

4. Geben Sie den aktuellen Code im Feld **Code eingeben** ein.

5. Geben Sie in den Feldern **Neuen Code eingeben** und **Code bestätigen** einen neuen Code ein und klicken Sie auf **OK**, um die Änderungen zu speichern.

TOOLTIPS ANZEIGEN

Während Sie die Einstellungen der Komponenten anpassen, zeigt Kaspersky Mobile Security 9.0 standardmäßig kurze Tooltips für die jeweilige Funktion an. Die Anzeige von Tooltips für Kaspersky Mobile Security 9.0 lässt sich anpassen.

Gehen Sie folgendermaßen vor, um die Anzeige von Tooltips anzupassen:

1. Gehen Sie auf **Menü** → **Erweitert**.

   Das Fenster **Erweitert** wird geöffnet.

2. Gehen Sie auf **Einstellungen**.

   Das Fenster **Einstellungen** wird geöffnet.

3. Gehen Sie auf **Tooltips**.

   Das Fenster **Tooltips** wird geöffnet.

4. Wählen Sie einen Wert für **Tooltips**:

   - **Anzeigen** – Tooltips anzeigen, bevor eine Funktion angepasst wird.
   - **Verbergen** – keine Tooltips anzeigen.

Abbildung 125. Anzeige von Tooltips anpassen

5. Klicken Sie auf **OK**.

AUDIOSIGNALE VERWALTEN

Bei der Arbeit des Programms treten unterschiedliche Ereignisse auf. Dazu zählen beispielsweise der Fund eines infizierten Objekts oder eines Virus, der Ablauf der Lizenz usw. Damit das Programm Sie über solche Ereignisse informiert, können Sie entsprechende Audiosignale aktivieren.

In der Grundeinstellung aktiviert Kaspersky Mobile Security 9.0 die Audiosignale nur entsprechend dem für das Gerät festgelegten Modus.

Verwenden Sie den Joystick oder die Navigationstasten des Geräts, um die Parameterwerte zu ändern.

Gehen Sie folgendermaßen vor, um die Audiosignale des Programms zu verwalten:

1. Gehen Sie auf **Menü** → **Erweitert**.

   Das Fenster **Erweitert** wird geöffnet.

2. Gehen Sie auf **Einstellungen**.

   Das Fenster **Einstellungen** wird geöffnet.

3. Gehen Sie auf **Ton**.

4. Das Fenster **Ton** wird geöffnet.

5. Wählen Sie einen Wert für **Audiosignale** (s. Abb. unten):

   - **Aktivieren** – unabhängig vom Geräteprofil immer Audiosignale verwenden.
   - **Deaktivieren** – keine Audiosignale verwenden.

Abbildung 126. Audiosignale verwalten

6. Klicken Sie auf **OK**, um die Änderungen zu speichern.

KONTAKTAUFNAHME MIT DEM TECHNISCHEN SUPPORT

Wenn Sie Kaspersky Mobile Security bereits erworben haben, werden Sie per Telefon oder über das Internet von den Spezialisten des technischen Supports unterstützt.

Die Support-Spezialisten beantworten Ihre Fragen zur Installation und Verwendung des Programms und helfen Ihnen dabei, die Folgen von Virenangriffen zu beheben, wenn Ihr Computer infiziert wurde.

Bitte lesen Sie die Supportrichtlinien (http://support.kaspersky.de/support/rules), bevor Sie sich an den technischen Support wenden.

E-Mail-Anfrage an den Technischen Support

Zur Kontaktaufnahme mit dem Technischen Support dient ein Kontaktformular (http://www.kaspersky.com/de/kontakt).

. Machen Sie in den obligatorisch auszufüllenden Feldern folgende Angaben:

- **Name und E-Mail**. Geben Sie hier bitte ihren vollständigen Namen und ihre E-Mailadresse an
- **Name und Versionsnummer des Programms**.
- **Betriebssystem**. Geben Sie die Kundennummer und das Kennwort an, die Sie bei der Anmeldung auf der Webseite des Technischen Supports erhalten haben.
- **Lizenztyp**. Geben Sie hier bitte an, ob sie eine Voll- oder Testversion besitzen
- **Problemart.** Wählen Sie hier bitte aus der Liste die zutreffendeste Problemart aus
- **Problembeschreibung**. Beschreiben Sie das Problem möglichst genau.

Technischer Support am Telefon

Bei dringenden Problemen können Sie Ihren lokalen technischen Support anrufen. Wenn Sie sich an den deutschsprachigen (http://www.kaspersky.de/technischer_support) oder internationalen (http://support.kaspersky.de/support/international) Support wenden, halten Sie bitte die Informationen (http://support.kaspersky.com/de/support/details) über Ihr Gerät und das installierte Antiviren-Programm bereit. Dadurch können unsere Spezialisten Ihnen möglichst schnell helfen.

GLOSSAR

A

ARCHIV

Datei, die ein oder mehrere Objekte "enthält", die ihrerseits auch Archive sein können.

D

DATEIMASKE

Platzhalter für den Namen und die Erweiterung einer Datei, der aus allgemeinen Zeichen besteht. Die beiden wichtigsten Zeichen in Dateimasken sind * und ? (wobei * für eine beliebige Anzahl von Zeichen steht und ? für ein beliebiges Einzelzeichen). Mit Hilfe dieser Zeichen kann jede beliebige Datei dargestellt werden. Beachten Sie, dass Name und Endung einer Datei stets durch einen Punkt getrennt werden.

DATENBANKEN

Die Datenbanken werden von den Kaspersky-Lab-Spezialisten erstellt und enthalten eine detaillierte Beschreibung aller im Moment existierenden Bedrohungen für die Computersicherheit und der dafür notwendigen Erkennungs - und Desinfektionsmethoden. Die Datenbanken werden von Kaspersky Lab laufend aktualisiert, wenn neue Bedrohungen auftauchen. Um die Qualität der Erkennung von Bedrohungen zu steigern, wird empfohlen, die Updates der Datenbanken regelmäßig von den Kaspersky-Lab-Updateservern herunterzuladen.

DESINFEKTION VON OBJEKTEN

Verarbeitungsmethode für infizierte Objekte, bei der die Daten vollständig oder teilweise wiederhergestellt werden oder sich ergibt, dass eine Desinfektion unmöglich ist. Objekte werden auf Basis von Datenbank-Einträgen desinfiziert. Beim Desinfektionsvorgang können Daten teilweise verloren gehen.

G

GÜLTIGKEITSDAUER DER LIZENZ

Zeitraum, für den Sie berechtigt sind, alle Funktionen des Kaspersky-Lab-Programms zu nutzen. Die Gültigkeitsdauer einer Lizenz beträgt in der Regel ein Kalenderjahr ab der Installation der Lizenz. Wenn die Lizenz abgelaufen ist, wird die Funktionalität des Programms eingeschränkt: Das Update der Datenbanken ist nicht mehr möglich.

I

INFIZIERTES OBJEKT

Objekt, das schädlichen Code enthält: Bei der Untersuchung des Objekts wurde erkannt, dass ein Abschnitt des Objektcodes vollständig mit dem Code einer bekannten Bedrohung übereinstimmt. Die Kaspersky-Lab-Spezialisten warnen davor, mit solchen Objekten zu arbeiten, da dies zur Infektion Ihres Geräts führen kann.

N

NICHT-ZIFFERN-NUMMERN

Eine Nicht-Ziffern-Nummer (auch Buchstabenwahl-, Wortwahlrufnummer oder Vanity-Rufnummer) ist eine Telefonnummer, die teilweise oder vollständig aus Buchstaben besteht.

O

OBJEKT BLOCKIEREN

Der Zugriff auf ein Objekt wird für externe Programme verboten. Ein blockiertes Objekt kann nicht gelesen, ausgeführt, verändert oder gelöscht werden.

OBJEKT LÖSCHEN

Verarbeitungsmethode für ein Objekt, bei der das Objekt physikalisch von dem Ort gelöscht wird, an dem es vom Programm gefunden wurde (Festplatte, Ordner, Netzwerkressource). Diese Verarbeitungsmethode wird für gefährliche Objekte empfohlen, deren Desinfektion nicht möglich ist.

P

PROGRAMM AKTIVIEREN

Bei der Programmaktivierung wird nach der Eingabe eines Aktivierungscodes ein Schlüssel heruntergeladen, mit dem das Programm die vorliegenden Nutzungsrechte und die Gültigkeit der Lizenz prüft.

Q

QUARANTÄNE

Die Quarantäne ist ein besonderer Ordner, in den alle möglicherweise infizierten Objekte verschoben werden, die während der Untersuchung des Geräts oder im Laufe des Echtzeitschutzes erkannt werden.

QUARANTÄNE (OBJEKTE IN DIE QUARANTÄNE VERSCHIEBEN)

Verarbeitungsmethode für ein möglicherweise infiziertes Objekt. Dabei wird der Zugriff auf das Objekt gesperrt und das Objekt wird vom ursprünglichen Ort in den Quarantäneordner verschoben. Dort wird es in verschlüsselter Form gespeichert, um eine Infektion auszuschließen.

S

SMS-NACHRICHTEN LÖSCHEN

Verarbeitungsmethode für SMS-Nachrichten, die Spam-Merkmale aufweisen. Dabei wird die Nachricht physikalisch gelöscht. Diese Methode wird für SMS-Nachrichten empfohlen, die eindeutig als Spam gelten.

SCAN AUF BEFEHL

Funktionsmodus von Kaspersky-Lab-Programmen, der vom Benutzer initiiert wird und der Untersuchung bestimmter Dateien dient.

SCHWARZE LISTE

Die Einträge dieser Liste enthalten:

Telefonnummern, von denen eingehende Anrufe und SMS durch Anti-Spam blockiert werden, und an die ausgehende Anrufe und SMS durch die Kindersicherung blockiert werden.

Text, bei dessen Fund eine eingehende SMS blockiert wird.

U

UPDATE

Bei einem Update werden alte Dateien (Datenbanken oder Programm-Module) durch neue ersetzt oder es werden neue Dateien hinzugefügt. Die neuen Dateien werden von den Kaspersky-Lab-Updateservern heruntergeladen.

W

WEISSE LISTE

Die Einträge dieser Liste enthalten Telefonnummern, von denen eingehende Anrufe und SMS durch Anti-Spam erlaubt werden, und an die ausgehende Anrufe und SMS durch die Kindersicherung erlaubt werden, oder Text, bei dessen Fund eine eingehende SMS übersprungen wird.

WIEDERHERSTELLUNG

Ein Originalobjekt wird aus der Quarantäne oder aus dem Backup entweder an den ursprünglichen Ort, an dem das Objekt gespeichert war, bevor es in die Quarantäne verschoben, desinfiziert oder gelöscht wurde, oder in einen benutzerdefinierten Ordner verschoben.

KASPERSKY LAB

Kaspersky Lab wurde 1997 von Eugene Kaspersky gegründet und befindet sich bis heute in Privatbesitz. Das Unternehmen mit Hauptsitz in Moskau beschäftigt weltweit über 1.700 hochspezialisierte Mitarbeiter, davon mehr als 140 in der deutschen Niederlassung in Ingolstadt. Rund um den Globus entwickeln die Virenexperten seit Jahren zuverlässige, innovative IT-Sicherheitslösungen zum Schutz vor Viren, Hackern und Spam.

Über 250 Millionen Anwender vertrauen weltweit auf die Produkte und Services von Kaspersky Lab. Diese haben sich durch schnelle Reaktionszeiten und hohe Erkennungsraten international einen Namen gemacht. Zahlreiche unabhängige Tests bestätigen die hohe Qualität der Lösungen von Kaspersky Lab.

Für den bestmöglichsten Schutz forscht Kaspersky Lab ständig an neuen Technologien und ist dabei ein wichtiger Wegbereiter für neue Sicherheitsstandards. So hat Kaspersky Lab nicht nur als erster Hersteller auf einen proaktiven Schutz vor unbekannten Viren gesetzt, sondern auch den ersten Virenschutz für Linux entwickelt sowie die erste Antiviren-Lösung mit Citrix-Zertifikat auf den Markt gebracht.

Innovative Technologien

Kaspersky Lab zählt weltweit zu den führenden Unternehmen beim Schutz vor Viren, Hackern und Spam. Über das Kaspersky Security Network erhalten unsere Experten täglich über 25 Millionen verdächtige Viren-Samples in Echtzeit zur Analyse. Dadurch reagiert das hoch spezialisierte Virenlabor meist am schnellsten auf neue Bedrohungen.

Innovative Technologien wie die proaktive Analyse von Bedrohungen schützen Anwender auch vor unbekannten Gefahren aus dem Internet, und das bei minimalem Ressourcenverbrauch.

Produkte & Services

Mit den erfolgreichen Heimanwender-Produkten Kaspersky Anti-Virus und Kaspersky Internet Security zählt Kaspersky Lab zu den führenden Unternehmen in Deutschland.

Ebenso sichern eine Vielzahl an Unternehmen und öffentlichen Einrichtungen jeder Größe ihre komplette IT-Infrastruktur mit individuell angepassten Kaspersky-Lösungen ab. Neben zentraler Installation und Administration zeichnen sich unsere Unternehmenslösungen vor allem durch hohe Erkennungsraten, schnelle Reaktionszeiten auf neue Bedrohungen und niedrigen Ressourcenverbrauch aus.

Mit den Hosted Security Services erhalten Sie die Sicherheit von Kaspersky Lab auch als Managed Service.

Webseite von Kaspersky Lab:	www.kaspersky.de
Viren-Enzyklopädie:	www.viruslist.de
Kontakt:	http://www.kaspersky.de/kontakt
Technischer Support:	http://support.kaspersky.de
Feedback zu unseren Benutzerhandbüchern:	docfeedback@kaspersky.de
Antiviren-Labor:	newvirus@kaspersky.com (nur zum Einsenden verdächtiger Objekte, die zuvor archiviert wurden)

CRYPTOEX OOO

Für die Überprüfung elektronischer digitaler Signaturen wird in Kaspersky Mobile Security die Krypto-Bibliothek (Programmbibliothek zum Informationsschutz - PBSI) "Crypto C" verwendet, die von CryptoEx OOO entwickelt wurde.

Webseite von CryptoEx OOO: http://www.cryptoex.ru

SACHREGISTER

A

Aktionen
- Virensuche ... 46, 136

Aktionen für Objekte ... 40, 46, 129, 136

Aktivieren
- Anti-Spam ... 53, 141
- Firewall ... 91, 180
- Kindersicherung ... 65, 153
- Privatsphäre ... 172
- Verschlüsselung ... 94, 182

Anti-Spam
- Aktion für Anruf ... 63, 151
- Aktion für Nachricht ... 62, 150
- Kontakte, die nicht im Telefonbuch stehen ... 60, 148
- Modi ... 53, 141
- Nicht-Ziffern-Nummern ... 61, 149
- Schwarze Liste ... 54, 142
- Weiße Liste ... 57, 145

Archive
- Virensuche ... 48, 134

Ä

Ändern
- Liste der geschützten Kontakte für die Privatsphäre ... 88, 177
- Schwarze Liste der Kindersicherung ... 68, 156
- Schwarze Liste für Anti-Spam ... 56, 144
- Weiße Liste der Kindersicherung ... 71, 159
- Weiße Liste für Anti-Spam ... 59, 147

B

Befehl senden ... 81, 170

Bildschirm
- Fenster für den Schutzstatus ... 34, 124
- Hintergrundbeleuchtung ... 106
- Schutzsymbol ... 34, 108

C

Code
- Aktivierungscode ... 23, 114
- Geheimcode ... 27, 117

D

Daten
- Entschlüsselung ... 95, 183
- mit Code blockieren ... 96, 185
- Verschlüsselung ... 94, 182
- vertrauliche Daten ... 82, 171

Datenzugriff blockieren ... 96, 185

Deaktivieren
- Anti-Spam ... 53, 141
- Kindersicherung ... 65, 153
- Privatsphäre ... 83, 172
- Verschlüsselung ... 95, 183

Diebstahlschutz
- GPS-Find ... 79, 168

SIM-Watch ... 78, 167
SMS-Block ... 73, 162
SMS-Clean ... 75, 163

E

Eintrag
Schwarze Liste für Anti-Spam ... 54, 142
Weiße Liste der Kindersicherung ... 70, 158
Weiße Liste für Anti-Spam ... 58, 146
Ereignisbericht ... 103, 191
Ereignisberichte
Einträge anzeigen ... 103, 191
Einträge löschen ... 104, 192
Erlauben
ausgehende Anrufe ... 69, 157
ausgehende SMS-Nachrichten ... 69, 157
eingehende Anrufe ... 58, 146
eingehende SMS-Nachrichten ... 58, 146
Netzwerkverbindungen ... 91, 180

F

Firewall
Sicherheitsstufe ... 91, 180
Firewall
Meldung über Verbindung ... 92

G

Geheimcode ... 27, 117

H

Hintergrundbeleuchtung ... 106
Hinzufügen
Liste der geschützten Kontakte für die Privatsphäre ... 87, 176
Schwarze Liste der Kindersicherung ... 66, 154
Schwarze Liste für Anti-Spam ... 54, 142
Weiße Liste der Kindersicherung ... 70, 158
Weiße Liste für Anti-Spam ... 58, 146

K

Kindersicherung
Modi ... 65, 153
Schwarze Liste ... 66, 154
Weiße Liste ... 69, 157

L

Lizenz ... 30, 120
Informationen ... 31, 121
Lizenzvertrag ... 30, 120
Programm aktivieren ... 23, 114
Verlängerung ... 32, 122
Lizenz verlängern ... 32, 122
Lizenzvertrag ... 30, 120
Löschen
Berichtseinträge ... 104, 192
Liste der geschützten Kontakte für die Privatsphäre ... 89, 178
Programm ... 19, 111
Quarantäneobjekt ... 51, 139
Schwarze Liste für Anti-Spam ... 57, 145
Schwarze Liste für die Kindersicherung ... 69, 157
Weiße Liste der Kindersicherung ... 72, 160

Weiße Liste für Anti-Spam ... 60, 148

M

Modi
- Anti-Spam ... 141
- Anti-Spam ... 53
- Kindersicherung ... 65, 153
- Privatsphäre ... 83, 172

N

Netzwerk
- Access Point ... 102

O

Objekt wiederherstellen ... 51, 138

P

Privatsphäre
- automatischer Start ... 84, 173
- ferngesteuerter Start ... 85
- Liste der geschützten Kontakte ... 87, 176
- Modi ... 83
- Schutzobjekte wählen ... 89, 178

Programm aktivieren
- Lizenz ... 30, 120

Programm aktivieren ... 23

Programm aktivieren ... 114

Programm installieren ... 18, 110

Programm-Menü ... 37, 126

Programmoberfläche ... 34, 124

Q

Quarantäne
- Objekt löschen ... 51, 139
- Objekt wiederherstellen ... 51, 138
- Objekte anzeigen ... 50, 138

R

Registerkarten des Programms ... 36

S

Schlüsseldatei ... 30, 121

Schutzstatus ... 34, 107, 124

Schutzsymbol ... 34, 108

Schwarze Liste
- Anti-Spam ... 54, 142
- Kindersicherung ... 66, 154

Sicherheitsstufe
- Firewall ... 91, 180

Sicherheitsstufe der Firewall wählen ... 91, 180

SMS-Block
- ausgehende Anrufe ... 66, 154
- ausgehende SMS-Nachrichten ... 66, 154
- Eingehende Anrufe ... 54, 142
- eingehende SMS-Nachrichten ... 54, 142
- verschlüsselte Daten ... 96, 185

Start
- Programm ... 28, 118

Update 99, 188
Virensuche 42, 131

T

Ton 105

U

Update
Access Point 102
Manuell starten 99, 188
Programmversion 22, 113
Roaming 101
Start nach Zeitplan 100, 189

V

Verbieten
ausgehende Anrufe 66, 154
ausgehende SMS-Nachrichten 66, 154
eingehende Anrufe 54, 142
eingehende SMS-Nachrichten 54, 142
Netzwerkverbindungen 91, 180
Verschlüsselung
automatisch blockieren 96, 185
Daten entschlüsseln 95, 183
Daten verschlüsseln 94, 182
Virensuche
Aktionen für Objekte 46, 136
Archive 48
Manuell starten 42, 131
Start nach Zeitplan 44, 133
Untersuchungsobjekte 45, 134

W

Weiße Liste
Anti-Spam 57, 145
Kindersicherung 69, 157

Z

Zeitplan
Update 100, 189
Virensuche 44, 133